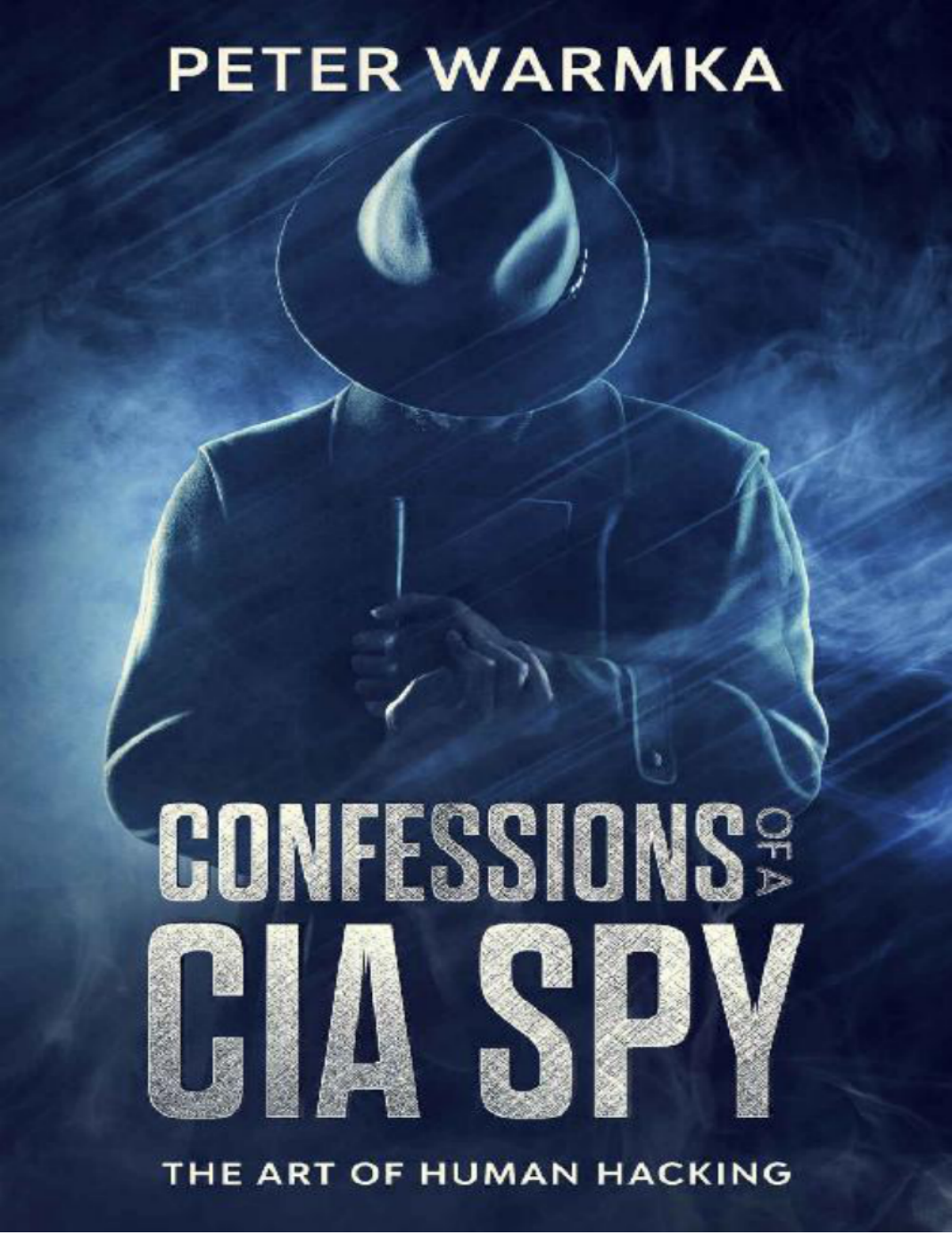
PETER WARMKA



CONFESSIONS OF A CIA SPY

THE ART OF HUMAN HACKING

Praise for Confessions of a CIA Spy

"A must-read for anyone who wants to protect themselves and their organizations from falling prey to manipulation tactics used by the world's savviest social engineers."
-- Michael Hayden, retired four-star general USAF, former Director of NSA and Director of the CIA, Principal at the Chertoff Group, author of New York Times bestseller *Playing to the Edge* and *The Assault on Intelligence.*

"Peter Warmka had an amazing career in the CIA and continues to use his expertise in the private sector. His new book Confessions of a CIA Spy: The Art of Human Hacking is the best guide I have seen on the new battleground of espionage. Cyber, social engineering, and human hacking have become the name of the game. You owe it to yourself to read this book to protect yourself and your organization from some highly sophisticated and devious attacks."
--James Olson, former Chief of CIA Counterintelligence, and the author of *To Catch a Spy: The Art of Counterintelligence.*

"You get what you negotiate' is a popular business phrase. However, in today's Wild West of cyber insecurity, a retired CIA officer offers sobering counter counsel: What you have, they are coming after. From decades of recruiting spies, Peter Warmka knows how to steal secrets, or more accurately, how to persuade people to give up their secrets. Confessions of a CIA Spy describes successful collection techniques, tricks if you will, that are used to steal far more than government classified material. These are subtle, crafted maneuvers which, to the uninitiated, appear like normal behavior, but are the very tools used to compromise your company's data and deplete your bank account. Readable, eye-opening and based on a deep knowledge of espionage tradecraft, Confessions of a CIA Spy reveals the playbook of those who prey on the unsuspecting. Warmka's work arms the reader with an awareness of the attacker's game plan. As a result, you win, they lose."
--Robert Wallace, Author of *Spycraft: The Secret History of the CIA's Spytechs from Communism to al-Qeeda* and executive producer of the Netflix series, *SPYCRAFT*.

“Peter Warmka provides a unique and very valuable perspective for companies and individuals on how to avoid cyber crimes. As a former CIA operative with deep experience penetrating the computer defenses of formidable adversaries, Peter is now on the other side of the equation, helping companies to learn from his experiences and to better protect themselves and their companies from cyber attacks.”
--Kevin Hulbert, former CIA Senior Executive, Member of the President’s Intelligence Advisory Board, President of XK Group

“In Confessions of a CIA Spy, Peter Warmka reveals espionage strategies that are used by nation states, criminal groups and multinational corporations every day to collect intelligence and/or steal secrets. The companies that choose to bury their head in the sand, believing that espionage is merely the purview of a country’s intelligence service, are not only wrong but place themselves at the mercy of unethical actors that could cost them millions of dollars. Readers of Peter’s book will not only understand how to prevent others from stealing their engineering secrets, market strategies and other proprietary data, it will demonstrate how to collect the information they need to have the competitive edge. Peter’s mastery of his craft and his gifts as a communicator has made him a sought-after trainer, and one that I not only trust, but highly recommend to all those interested in harnessing the power and efficacy of this proven methodology.”
--Michele Rigby Assad, former CIA Intelligence Officer, Consultant/ Trainer, and Author of *Breaking Cover: My Secret Life in the CIA and What it Taught Me About What’s Worth Fighting For*

"A very thorough and detailed account of the nature of the threats facing organizations today, from criminal organizations, malicious insiders and nation state actors. Peter delves deep into the sophistication that accompanies some of these adversaries who have in their sights the sensitive information housed within both corporations and governmental entities. Based upon his own experience in breaching security infrastructure, Peter offers insights to organizations about mitigation strategies. A great read."
--Brian W. Lynch, Executive Director, RANE; a retired FBI Agent, and former Head of Global Security for The Vanguard Group

“*Confessions of a CIA Spy - The Art of Human Hacking* comes from a CIA career spy whose lifetime of experiences led him to form the Counterintelligence Institute, which addresses security and intelligence issues in individual and company lives.
As such, readers might expect a series of spy stories from this book,

but it offers so much more. Herein lies the opportunity to understand the presence, effects, and processes of disinformation, hacking, and other intelligence hacks in daily citizens' lives. *Confessions of a CIA Spy* excels in identifying these problems and how to overcome them.
Information is a powerful tool. It can be successfully managed or artfully mismanaged, and the latter can be compromised more easily in this era than at any other point in human history.

Confessions of a CIA Spy reviews this process, and is especially powerful in its assessments of organizational security and implementing protections to address situations which at first might not seem to pose opportunities for disaster: "*While an entity may aggressively use social media to help promote their products and services, an unintended consequence can be the leakage of information, which can be invaluable to social engineers. This exposure results in the creation of vulnerabilities for the organization. Company employees will often upload photos or videos of themselves in the workplace to social media sites, providing social engineers with insight into their physical workspaces."*
The insights on how social engineers and information gatherers often don't even have to produce a bona fide hack to gain access to company data and details is positively frightening--as well as enlightening.
By understanding the extent and processes of hackers and how 'social engineers' manipulate both loopholes and emotions, companies and individuals who look to improve their security measures will find the many layers of hacking approaches intriguing. This will allow them to uncover gaps in company safety processes which they may not have considered previously, going beyond the usual emphasis on cybersecurity firewalls: The social engineer may place pressure upon the target by implying that refusing to assist will be seen by others as socially unacceptable...These influence techniques can be used in a variety of situations, including brief one-time interactions with a target. The wide-ranging, authority-backed discussions of various forms of hacking make *Confessions of a CIA Spy - The Art of Human Hacking* a key acquisition. While those who wanted true-life spy stories may be disappointed, ultimately, the focus on the extent of human hacking operations is both invaluable and intriguing, exposing scenarios of vulnerability that many will not have thought of before.
No cybersecurity or social issues collection should be without *Confessions of a CIA Spy."*

--D. Donovan, Senior Reviewer, Midwest Book Review

CONFESSIONS OF A CIA SPY

THE ART OF HUMAN HACKING

PETER WARMKA

Copyright © 2021 Peter Warmka

All rights reserved. No part of this book may be used or reproduced in any manner without written permission except in the case of brief quotations used with full credit and citation to the original work and author.

All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the U.S. Government. Nothing in the contents should be construed as asserting or implying U.S. Government authentication of information or endorsement of the author's views.

Cataloguing-in-Publication Data is on file with the Library of Congress.

ISBN PAPERBACK: 979-8-554614-5-45

Library of Congress Control Number: 2020924563

For my wife, Carmen, who has always supported my dreams and never given up on me.

Table of Contents

Acknowledgment

Foreword

Preface

Introduction fo the World of Manipulation

Chapter 1 - What We Want and How We
Rationalize Stealing

Chapter 2 - Collecting Information on a
Target Organization

Chapter 3 - Selecting Insiders and Collecting
Personal Assessment Data

Chapter 4 - Designing a Pretext for an Approach

Chapter 5 - Leveraging Psychology for Manipulation:
Trust and Influence Factors

Chapter 6 - The Art of Elicitation

Chapter 7 - Channels for Manipulation
The Art of Phishing and Smishing

Chapter 8 - Chaannels for Manipulation:
The Art of Vishing and Face-to-Face Encounters

Chapter 9 - How Organizations Can Mitigate the
Risk of a Security Breach

Chapter 10 - Taking it Home: Safeguarding your
Personal Information and Financial Security

Chapter 11- The Future of Human Hacking

Appendix A - Personal Assessment Questionaire

Appendix B - Additional Resources

Glossary

About the Author

Contents

Praise for Confessions of a CIA Spy
Title Page
Copyright
Dedication
Table of Contents
Acknowledgements
Foreword
Preface
Introduction to the World of Manipulation
Chapter 1
Chapter 2
Chapter 3
Chapter 4
Chapter 5
Chapter 6
Chapter 7
Chapter 8
Chapter 9
Chapter 10
Chapter 11
Appendix A
Appendix B
Glossary
About the Author

Acknowledgements

This book would never have been published without the assistance and support of numerous people. David Quilter, whose pen authored the foreword, served as my principal mentor during my transition from federal service back into the private sector. Another mentor, Charles Saba, inspired me to pursue this passion and strongly encouraged that I take my message globally. Through the assistance of both Charles and Heital Yaagnik, I am in the process of organizing several virtual and in-person international events focused on counterintelligence and insider threats.

While too many to detail, there are dozens of friends and business associates who reviewed draft portions of this book providing their feedback, insights and words of encouragement. Thank you all!

I would be remiss to not acknowledge the support I received from my family during my career within the CIA. At the time of my first overseas deployment, only my spouse and father knew my true affiliation. I had to intentionally hold back the truth from remaining family members due to cover sensitivities. Only a couple of years prior to my retirement did I bring the rest of my family into the "circle of trust" like Robert De Niro in the 2000 film Meet the Parents. Fortunately, my confession was well received.

Of course, those who made the most sacrifices for me during my CIA adventure were my wife, Carmen, and our children Mary, Alexander and Chrissy. They continue to provide invaluable assistance in the validation of marketing ideas, proofing of draft communications and the development of social media content.

Finally, a very special mention goes to my superb editor, Lillian Chapa, who worked tirelessly in turning my rough manuscript into a book which hopefully will be enjoyed by many. She has already agreed to assist with my next effort.

Foreword

I have known Peter Warmka for more than 10 years, ever since we met through the Association of Certified Fraud Examiners, the global organization that combats embezzlement, fraud and theft of information of all types. We have both been Certified Fraud Examiners for more than 20 years, and since our first meeting we have been both friends and colleagues. I've long known and respected Peter as a consummate public servant and professional.

Confessions of a CIA Spy: The Art of Human Hacking is Peter's primer on the awareness you and I need when it comes to data, social media sites and information. Peter points out what not to do when it comes to anything and everything involved with electronic communications and publicly available information. From my perspective as the senior security executive at four Fortune 500 companies, a career with the U.S. Drug Enforcement Administration, and veteran of the Marine Corps—totaling more than five decades of experience—I immediately understood how valuable Peter's experience and expertise is in dealing with the broad spectrum of information management, and at times, mismanagement.

Having the responsibility and accountability for tens of thousands of employees and tens of billions of dollars in business assets around the world takes lifelong learning and colleagues like Peter. During our first meeting and ever since then, I have come to appreciate Peter's utmost honesty and his determination to share his life experience as a CIA undercover operative in very compelling ways: to always educate, enhance and protect the integrity of both individual and institutional information.

What I found in these pages are step-by-step levels of awareness and expertise that will help you better understand how we are frequently unaware of what can and often actually does happen to our personal information and identity.

As Peter aptly points out, it is important to remember that any information you are providing online about yourself, your family or your company makes you a potential target for any organization that can and will use your information for whatever purposes it wants. It is

all a part of the public domain.

From a business perspective, Peter provides what amounts to a must-read for IT professionals, HR managers, security professionals, C-suite executives and leaders at all levels. In addition, parents have a need to know about common social engineering schemes because all too often their family members have no awareness of their vulnerability. Peter shares rare and candid insight into a threat that so few people know even exists. He offers practical personal advice, including a Personalized Assessment Questionnaire that readers can use to assess how and where they themselves may be more vulnerable than they, their business or family want to be. This I find invaluable!

Through the COVID-19 pandemic and beyond, we understand that the economic downturn will lead to an inevitable increase in criminal activity, such as theft, fraud, burglaries, robbery and yes, breaches to steal valuable individual data. The “Human Hacker” has delivered this book to help us avoid and mitigate harm.

J. David Quilter has served as executive security leader at Baxter International, Allegiance Healthcare, Cardinal Health and NiSource. He is a life member of the International Security Management Association (ISMA) and is on the Emeritus Faculty of the Security Executive Council. He is the author of *From One Winnng Career to the Next*, now in its 2nd edition.

Preface

It was only upon leaving the Central Intelligence Agency (CIA) in 2010 and entering the private security industry that I learned there was a specific field called social engineering, also referred to as human hacking. Popular literature described it as a process by which someone manipulates humans in order to breach security, whether it be the security of the organization or the individual's personal security, and it generally carried a very negative connotation. Although I was just learning about the approach, I realized that I had spent much of my CIA career as an intelligence officer who, in fact, used social engineering skills quite effectively to accomplish my missions. It became a bit of a personal dilemma for me. Was the intentional manipulation of fellow human beings something inherently evil? Or was it simply a tool that could be used for evil as well as good? The more I thought about the topic, the more the passion stirred within me to analyze the methodology of social engineering and its impact upon the security of organizations as well as individuals.

In 2015, Webster University invited me to teach as an adjunct professor in their master's degree program for cybersecurity. While addressing intelligence and counterintelligence issues as they related to cyberwarfare, I decided to incorporate my knowledge and skills as a spy in explaining how individuals are effectively targeted and manipulated by adversaries using a variety of social engineering techniques.

What made my course truly impactful for my students was an assigned capture the flag social engineering project. Modeled somewhat after the annual Social Engineering Capture the Flag competition held during computer security conferences in Las Vegas, I assigned each of my students a U.S. corporate entity as their social engineering target. The purpose of the exercise was to collect as many flags as possible and develop a proposal for breaching the target entity's security. The flags were specific pieces of information that addressed potential exploitable vulnerabilities in a target's security system. Each student initially conducted Phase I open-source intelligence (OSINT) collection on their respective target by scouring a multitude of sites available on the World Wide Web. Once they demonstrated proficiency in OSINT collection and exhausted most of the available resources, I allowed them to move onto Phase II.

During Phase II, and under careful supervision, my students used information collected to formulate a variety of social engineering techniques to use against their target to gather additional flags. They concluded the project by detailing their Phase I and II processes, what information they were able to obtain, and possible recommendations for how they would pursue breaching the company's security. In addition to their academic paper, they presented their unique experience in the form of a presentation before the class. Without exception, students overwhelmingly completed the project with a much greater awareness regarding the threats posed by social engineering and how to help protect themselves as well as their respective organizations from such attacks.

In addition to my university platform, I began sharing this knowledge by writing articles for major trade publications as well as speaking at industry conferences focused on security, fraud and financial systems. While attendees were typically intrigued by social engineering and wanted to learn more, I found a severe deficiency in publicly available resources covering the topic. As a result, the general public continues to remain largely uninformed and completely susceptible to social engineering attacks delivered by phishing (email), smishing (SMS), vishing (telephone) or face-to-face interaction.

However, what is even more concerning is the general apathy of those who believe that they will never fall victim to such security breach attempts. This lack of concern is frequently found at all levels of the organization, including within the C-suite. Just as the ostrich puts his head in the sand believing that he will be protected from unseen threats, corporate leaders also harbor a false sense of security.

Unfortunately, this apathy and lack of understanding plays perfectly into the hands of cybercriminals when we consider that according to Verizon's 2020 Data Breaches Investigations Report (DBIR), more than 90 percent of successful breaches begin with social engineering. It was for this reason that I decided to establish the Counterintelligence Institute. My mission is to assist corporations, nonprofit organizations, academic institutes and city, state and federal government offices in the protection of their proprietary information and personal data records against security breach attempts initiated by social engineering. Through security awareness training, I focus on transforming the human factor from being the weakest link in security to becoming the most effective defensive tool against such threats.

While client organizations and their employees benefit from these training programs, my intention with writing this book is to be able to help all individuals understand these threats and to improve their security practices both at home and in the workplace. Whether you are a CEO of a major corporation, a dentist, a teacher, a homemaker

or retiree, this information is relevant to you.

To help provide a greater understanding of social engineering methodology, I showcase numerous examples throughout this book. While some of the stories may be fictionalized, the methodologies described throughout all these examples are very real.

As a former spy, I know that deception and manipulation can be very powerful forces. Denying that they exist will only increase their power over you.

Introduction to the World of Manipulation

Operation Samba

Sao Paulo, Brazil
16 April 2017

It had been two months since his last visit. Jean Claude checked into his usual hotel in Sao Paulo and reviewed the brief he had received two days ago. While the requirement was standard—penetrate a target entity and steal vital intelligence—each mission offered unique challenges, along with an assortment of associated risks.

His career as an intelligence operative had started in 1985 when he joined France's Directorate-General for External Security (DGSE), where he was trained to target both national governments and private companies. He was proud to serve his country by securing intelligence for the French government and, by extension, French multinational organizations that hungered for information that allowed them to always maintain a competitive edge. Since his retirement nearly five years earlier, Jean Claude had steady work as a freelancer in the world of industrial espionage—his expertise was in high demand.

This most recent client was interested in securing the program for XENOX 2000, a new software product that Brazilian firm COMTEC was planning to introduce into the marketplace by early next year. The client had already obtained some initial intelligence regarding these plans during a discussion with a software marketing representative at a conference.

At a very minimum, Jean Claude had to find a way to penetrate COMTEC and steal a copy of this program. The client had a buyer who wanted to develop the same product at a much cheaper cost and hopefully beat COMTEC's launch of the product to the market. A secondary requirement was to implant malware that would modify source code in COMTEC's program, causing it to fail shortly after its installation on the end user's server.

Jean Claude needed to learn about the organizational structure of

COMTEC to determine who within the company might have direct access to information regarding product development. His first instinct was to go online to visit the company's website, but it did not provide any useful names or contact information for personnel other than the front office.

Jean Claude next went to LinkedIn to search under "COMTEC" for any employees. While no one surfaced who was a current employee, there was one individual, Luisa Martins, who had previously worked as an administrative assistant in COMTEC prior to taking an administrative position with LUMANEX. In addition to these positions, Luisa listed her academic background and other professional interests. While not currently at COMTEC, Luisa would likely be able to provide considerable information regarding her former employer and be less inhibited than if she currently worked there.

Using an alias, Jean Claude decided to directly telephone LUMANEX and ask for Luisa. He identified himself as an HR consultant who found her profile on LinkedIn and was looking for someone with Luisa's background. Would she be willing to have lunch the following day to explore the potential employment opportunity? Luisa, flattered and full of curiosity, immediately accepted the invitation.

Meanwhile, Jean Claude pulled up Google Earth to look at COMTEC and the immediate vicinity. It appeared to be located directly across the street from the financial service firm PROVOX. Jean Claude picked up the telephone, called COMTEC's main switchboard and asked to speak with the person responsible for general maintenance. He was immediately transferred.

Hello, can I help you?

Yes, I really need some help. Are you in charge of maintenance?

Yes, this is Lucas. How can I assist?

I'm Gerardo from PROVOX across the street, your neighbor. I shouldn't say this but the cleaning company we use is not reliable. I want to see if we can find a better service provider. Are you happy with the company providing you with this service?

Yes, indeed. They are very reliable and efficient.

Wonderful, what's their name?

DELTA.

How often do they come per week?

Nightly around 8 p.m.

Maybe we could try them out. What's the name of the crew chief?

Everyone refers to him as Bruno. I have not seen him in a while as I'm usually out of here by 6 p.m.

I don't blame you. There is more to life than working! Thanks so much for your help. I will contact DELTA directly.

You are so welcome. Good luck.

Using a new alias, Jean Claude later called COMTEC's switchboard, claiming to work for the American-Brazilian Chamber of Commerce. He advised that they were planning an upcoming cybersecurity event and wanted to invite the head of COMTEC's security department as an attendee. The switchboard operator readily identified Robert Resende as holding this position. Jean Claude expressed his gratitude for the assistance and stated that he would forward the invitation by mail.

Later that evening, Jean Claude passed by the offices of COMTEC at exactly 8 p.m. and spoke with the night watchman. He requested to speak with Bruno from DELTA, who came highly recommended to him. Within ten minutes, Bruno appeared.

Hello Bruno. My name is Winston Bosquet and I work for Stedman Security. We are under contract by COMTEC's head of security, Robert Resende, to conduct a survey of how COMTEC's employees properly follow security practices in the handling of sensitive information. Mr. Resende does not want anyone in COMTEC to know about his special project, but he told me that you are someone whom I could completely trust.

What exactly do you need?

I would like to sit down with you over coffee to discuss your observations regarding how COMTEC employees protect their information. Do they leave things out on top of their desks? Leave computer passwords on sticky-notes? Leave file cabinet drawers unlocked? Shred sensitive documentation?

Bruno readily agreed to discuss these issues over coffee that same night. Jean Claude paid him R200 ($50) for 20 minutes of his time—and then asked for one more thing. Could Bruno consolidate and place COMTEC's trash in an area where Jean Claude could retrieve it over the next four days? If so, Jean Claude would pay him R1,000 ($250) upfront for this assistance. Bruno immediately jumped upon this opportunity for the additional income.

Several intact documents were retrieved by Jean Claude over the four days of collection. One was a complete internal personnel directory identifying departments, positions, names and contact information. The other was a draft slideshow presentation regarding the capabilities of the new software product. Overall, the investment in trash paid dividends.

Jean Claude then met Luisa for lunch, where he explained his work recruiting employees for a client who was setting up a new IT firm. Luisa was one of several people he wanted to meet to see if there might be a good fit. Over the next hour, Jean Claude poured on his charm by complementing Luisa on many facets of her personal and professional life. Under the pretext of potentially wanting to look at

COMTEC employees as additional candidates, Jean Claude was able to acquire information on key personalities there.

Obtaining the personnel directory in advance of this meeting was very beneficial. Of the 10 individuals who worked in the programming department, one appeared to be a very attractive target. His name was Sunjay Kumar, and Luisa described him as an Indian national who arrived in Sao Paulo two years ago. She depicted Sunjay as very well-mannered and a hard worker, but he missed his family back home and was having a hard time adjusting to life in Brazil. Most importantly, he was not very happy at COMTEC. He did not have a very good relationship with his department head. Luisa commented that Sunjay confided to her several months ago that he hoped to find other employment in Brazil or return back to India. For Jean Claude, this was very valuable insight. He concluded the meeting by telling Luisa that he would get back in contact when it was time to hire, and requested that she keep their conversation strictly confidential.

The next day Jean Claude telephoned COMTEC asking for Sunjay Kumar. Without going into details, Jean Claude said he was with the firm AVANTE and wanted to meet for dinner regarding a potential employment opportunity—Sunjay came highly recommended by a former employee of COMTEC. Although a bit hesitant, Sunjay agreed to meet Jean Claude for dinner at the exclusive Intercontinental Hotel, which had been chosen to impress Sunjay.

After exchanging pleasantries, Jean Claude explained that he worked for a consultancy firm located in Quebec, Canada. To alleviate any possible suspicion, Jean Claude provided Sunjay with a professional business card. While AVANTE only existed on paper, Jean Claude made sure to backstop any telephone calls made using a virtual account established through a business service center. Jean Claude explained to Sunjay that their main clientele were financial service firms located worldwide. In addition to assisting with their IT requirements, AVANTE also provided headhunting services to these clients. Currently, he was recruiting key personnel for a client that would be expanding their operations into Brazil.

Sunjay had come to Jean Claude's attention as a potential candidate, and he wanted to learn more about Sunjay's background. If found to be a potential fit, he would provide Sunjay with more specifics—the unidentified client did not want it publicly known that they were planning to enter the marketplace.

Sunjay spent the next couple of hours detailing his personal and professional background, including his work experience at COMTEC and his work on a project called XENOX 2000. While being careful not to complain about his office environment, Sunjay did mention that he was looking to advance in his career, whether in Brazil or another

country.

Following the dinner, Jean Claude reached out to a colleague he wanted to bring in to play the role of the prospective client. Barry, who was of Indian descent, flew into Sao Paulo for a day of rehearsals with Jean Claude. After getting Sunjay to sign a nondisclosure agreement, Jean Claude introduced "Pankaj" to Sunjay as head of the overseas expansion project for Indian IT giant PTU DATA. Fully familiar with Indian customs and speaking in Sunjay's native Punjabi, Pankaj was able to quickly establish rapport with Sunjay. Pankaj laid out the ostensible plan for opening offices in Brazil and stated that Sunjay was one of three people he was considering for the role of programming manager. In such a capacity, Sunjay would oversee a staff of 15 people and expect to earn twice his current salary, in addition to annual bonuses.

Sunjay sat on the edge of his seat—this position sounded like a chance of a lifetime. He wondered to himself whether he would be chosen over the other two candidates, but Pankaj added that Sunjay was a strong preference given his Indian background that would facilitate his ability to work with more senior PTU DATA managers. While everything looked good on paper, Pankaj needed to see an example of Sunjay's best programming work. Sunjay would need to provide a copy of the software program he was currently working on. If Sunjay was not ultimately offered the position, he would still be paid R50,000 ($12,500) for the program.

Sunjay justified his decision to assist Pankaj for several reasons. He saw this as a golden opportunity to move up in his career and felt personal satisfaction in helping a company from his homeland. He wanted to get back at his boss, who did not appreciate his hard work and potential, and the R50,000 would allow him to pay off some debts.

Sunjay used a special storage media device Pankaj had passed to him to download the program from COMTEC, but it also surreptitiously uploaded the malware with the altered code. Jean Claude got the USB from Barry and provided the program to his client, for which he was handsomely rewarded. After numerous customer complaints and significant bad press regarding XENOX 2000 and technical failures, another firm launched a very similar product and took the market by storm. Sunjay, who received his R50,000, was never contacted again.

Chapter 1

Threat Actors: What We Want and How We Rationalize Stealing

"The Chinese government does not engage in theft of commercial secrets in any form, nor does it encourage or support Chinese companies to engage in such practices in any way."

—Xi Jinping

As a child, I was raised in a very strict Catholic family. My parents made every effort to ensure that my five siblings and I were properly educated in the Catholic faith and dutifully practiced teachings focused on honesty, loyalty and philanthropy in our daily lives. At the age of 14, I left home to enter St. Lawrence Seminary, which prepares young men for possible vocations into the priesthood. My four years at the central Wisconsin seminary provided great opportunity for personal growth and reflection, and I was most impacted by summer mission trips to the east coast of Nicaragua. Even though I eventually decided to leave seminary studies, these mission experiences left me with a strong desire to someday work in Latin America.

Several years later, after obtaining my master's degree in international business management, I landed a position with a South Florida bank with operations throughout Latin America. My focus was on private banking, managing the accounts of high net-worth clients from various South American countries including Argentina, Brazil, Chile and Colombia.

During my time in this role, I learned that a successful private banker is one who excels at maintaining close and trusting relationships with clients. If the clients like you, your network will easily grow through referrals provided to their family members, friends and business associates. After establishing a roster of close working relationships, I moved on from private banking and began to work as a personal investment and security advisor to several clients.

Due to my frequent travel to Latin America, my network of contacts and fluency in Spanish and Portuguese, I was eventually approached by the Central Intelligence Agency (CIA). While I had never contemplated working for the U.S. government, let alone the CIA, I was intrigued and willing to explore the opportunity. They

wanted me to become a case officer, collecting foreign intelligence information to be used by U.S. officials to make better informed policy decisions. This information was non-public, sensitive and invaluable. The CIA would provide me with the intelligence requirement and identify who within an organization would likely have access to it. My job would be to gain access to such a person and eventually manipulate them into providing this information to me. In essence, I would learn how to creatively breach the security of a target organization to steal their most precious secrets. Such organizations would include various government ministries, senior government leadership circles and strategic state infrastructure. After several weeks of reflection, I made the decision to join the CIA.

You may think it peculiar for someone who seriously considered entering the priesthood to instead take a job with the underlining requirement to lie and steal. Truthfully, it was an initial moral conundrum for me. However, I was eventually able to rationalize it—I believed that this approach was the only way to successfully complete the mission, an undertaking that would be of ultimate service to my country.

During my career with the CIA, I learned the intricacies of befriending strangers, manipulating people through electronic communication and meticulously studying human behavioral patterns. The approaches I used—which I later understood to be social engineering—are practiced by all kinds of people, from the eager salesperson to the nation-state hacker.

I bring up my personal story to emphasize the variety of threat actors behind today's security breaches—who they are, what they are after and what drives them. Threat actors can be broken down into the following categories: state actors, organized criminal groups, industrial competitors, activist groups and malicious insiders.

State Actors

Practically every nation state in the world has an intelligence apparatus that strategically collects intelligence for both defensive and offensive purposes. The most active nations in information gathering include China, Great Britain, France, Iran, Israel, North Korea, Russia and the United States.

While the U.S. intelligence community does not typically collect information on commercial companies overseas, many foreign intelligence services do target U.S. corporations. They are trying to steal technology by acquiring intellectual property. Advancements in technology typically require years of research and significant development costs. If they can effectively steal such technology, they can save considerable time and money while propelling their respective industries to better compete with U.S. companies. China is

the most notorious for this.

Another area of focus by some state actors in conducting data breaches is gaining access to a target entity's customer or personnel data. Just as large companies such as Facebook and Google build databases on consumers to be used for marketing purposes, some state actors appear to be gathering detailed data on U.S. citizens for potential exploitation in future intelligence operations.

Many Americans received their personal wakeup call when they learned about the security breaches suffered in 2014 and 2015 by the Office of Personnel Management (OPM). OPM is the repository of personal information collected and analyzed by the U.S. government prior to issuing an individual with a security clearance. There is no single database in the world that has more information on the millions of U.S. citizens it contains. Approximately 21.5 million current and former federal employees received a letter from OPM advising that their personal information was breached, but all they were offered in return was a free service to monitor their online identity and credit reports.

A second notable security breach occurred at the credit bureau Equifax in 2017. Here, the hackers were able to gain access to the sensitive credit information of nearly 150 million Americans. Contrary to many smaller breaches where consumer credit card account information is sold through the underground market on the dark web and then used for identity theft or to gain access to other websites, the information acquired in the Equifax breach, as of this writing, has not surfaced. Cybersecurity experts believe that this information was not stolen for criminal activity, but rather by a foreign nation state for intelligence purposes.

According to U.S. intelligence experts, China was behind both breaches, which calls into question their objective. Was it to steal information to conduct identity theft, or is it for something much, much bigger? Think about the value of this information to a state actor such as the Chinese. The OPM data specifically relates to individuals who have access to U.S. intelligence secrets. Such information provides an intelligence service invaluable insight into motivations and vulnerabilities of these individuals that could be leveraged when trying to recruit them as potential intelligence sources. While the information stolen from Equifax is not as broad as that taken from OPM, it does identify individuals who are experiencing financial difficulties. Combining data from OPM along with Equifax would be extremely valuable to such an intelligence service.

Beyond OPM and Equifax, I would be remiss not to highlight that the industry with the greatest number of ongoing security breaches is

healthcare. If your healthcare provider or insurer was one of the thousands that have suffered breaches over the past several years, what data was potentially collected on you by the perpetrator of the crime? Your biographic history, your health history, employment details, social security number or credit card numbers could have been compromised. How could this information be used by someone with nefarious intent? While there is no evidence that China is behind the breaches in the healthcare industry, such information is dangerously powerful in the hands of any intelligence service.

Regardless of the ultimate collection goals sought by state actors when breaching security and stealing information, their intelligence officers are predominantly motivated by extreme loyalty to their country—it is seldom about money. Just like U.S. intelligence operatives, state actors risk discovery and potential incarceration in a foreign land.

Organized Crime

The vast majority of security breaches, including cyberattacks, can be attributed to criminal groups. Whether it's a small band of criminals or part of a large criminal syndicate, the motivation is predominantly financial gain. Think of them like art thieves—they generally do not steal works of art for their own collections but instead look to sell them on the black market. The biggest market for stolen digital information on the internet is the dark web.

Visualize the internet as an iceberg. At the very top, above the water's surface, is an area seen and accessed by Google and other search engines. This layer, commonly referred to as the surface web, represents just 5 percent of the entire internet. The other 95 percent beneath the surface is referred to as the deep web and contains locations that are not indexed and therefore not accessible by standard search engines. Within this deep web exists markets where criminals buy and sell information, as well as other products and services, while remaining anonymous and utilizing digital currencies.

While a significant portion of breaches may indeed be conducted by criminal elements, it is difficult to separate these attacks from those planned or orchestrated by nation states. In some cases, nation states will use organized criminal groups as a force multiplier in undertaking such actions while also deflecting attribution away from the nation state. Additionally, organized crime may approach nation states as potential clients for stolen data.

Beyond stealing data for internal use or resale, criminals will also target entities through other tactics. One of the most popular criminal schemes is ransomware, where the criminal breaches security to encrypt the target's data and hold it hostage. In return for the payment of the ransom, usually in the form of bitcoin, the criminal

will provide the victim with a decryption code. Once infected with ransomware, victims have few options. Unless they have previously installed a well-isolated data backup system with regular updates, the loss of access to their data practically paralyzes their operational activities, which can quickly result in substantial revenue loss. While government authorities typically recommend against paying the ransom, such a payment is usually much cheaper than suffering a shutdown of their business until their IT system and database can be rebuilt. For this reason, most victims end up paying the ransom. No organization or individual is safe from such attacks. They have hit small to large businesses, academic institutions and municipal, state and federal government offices as well as private individuals. According to a report by cybersecurity firm Emisoft, ransomware attacks cost the U.S. economy over $7.5 billion in 2019 and are predicted to only increase in the coming years.

Another increasingly popular tactic used by criminal groups in security breaches are business email compromise (BEC) schemes. This approach usually targets companies working with foreign suppliers as well as companies that regularly conduct wire transfers. In such cases, criminals are able to insert themselves in email correspondence between managers and those who might conduct wire transfers based upon their instructions. Posing as a manager, the criminal will send a well-crafted email providing urgent instructions to send a wire transfer to what appears to be a normal recipient. However, the specific wire transfer instructions are to a fraudulent bank account. Once the funds are received, the criminal quickly withdraws these funds before discovery. According to the U.S. Treasury, BEC attacks in 2018 were costing U.S. companies over $300 million per month.

Corporate Espionage

All corporations continuously collect information on their competitors to better position themselves within the marketplace. While competitive intelligence is predominantly collected within legal and ethical constraints, some companies will cross the line into unethical or illegal collection methods. At times, they may contract with intelligence operatives to distance themselves from such activity, failing to realize that discovery could result in serious criminal charges and a huge financial blowback to the corporation. More commonly, such firms will use recruitment techniques to hire new employees who agree to provide proprietary information they were privy to during their employment with a competitor firm.

Regardless of the technique deployed, the unlawful acquisition of corporate trade secrets is considered industrial espionage.

Activists

Activism may include efforts to advocate, block, direct or intervene

in political, social, economic or environmental reform with the goal of effecting changes in society. This activism can be expressed in numerous ways and may be either peaceful or violent. Peaceful measures include writing letters to politicians, placing op-eds in news publications, conducting public demonstrations or promoting boycotts. Escalated measures may invoke or promote acts of violence. On the extreme end of the spectrum are terrorist groups, which typically focus their efforts to invoke change through acts of terror. While governmental entities and officials were traditionally the main target for activist causes, more recent focus has been placed on major corporations. In such cases, activists attempt to pressure corporations to make changes that may affect the welfare of employees, the consumer or the environment.

Activist groups may try to breach the security of an entity to further their cause through methods such as stealing proprietary information for public disclosure in order to provide proof of accusations or to embarrass the entity. Frequently, such breaches end up seriously affecting the financial wellbeing of the firm. Other breaches may facilitate access into non-public or restricted spaces of the company for members of activist groups during planned protests.

Malicious Insiders

Threats are not always external to the enterprise—sometimes they develop from within. These insider threats usually stem from a disloyal employee of the firm who intends to personally benefit at the expense of the company. Such individuals are typically disgruntled and sometimes very angry. They may feel underappreciated, believing that they deserve a higher position or higher pay, or may feel belittled by their supervisor. In this case, revenge becomes a motivator, and they want to get back at their company. Another motivation may be financial. They may be suffering from financial duress, worried that they will not be able to support their family, or they may desire to afford certain luxuries in life.

Ultimately, such insiders will breach security protocols to obtain and use proprietary information for their own benefit. Some insiders may offer to sell the information to third parties, such as competitors or vendors trying to gain contracts with the company. The most frequent way insider threats come to fruition is when existing employees take proprietary information to establish their own businesses or to enhance their position with a new employer.

A subcategory within the insider threat is a whistleblower, an insider who decides to disclose sensitive information to government authorities or to the general public. It usually involves serious financial fraud or a coverup by management of a process or procedure that is considered detrimental to consumers. The whistleblower is

usually motivated by a desire to correct what they believe to be a serious wrong within the organization where they work. Like an activist, they want to effect change.

◆◆◆

Despite the threats outlined above, I frequently encounter individuals who believe that their organization will not become a target of interest, especially to foreign intelligence services or organized criminal groups. They believe their organization has nothing of real value to steal. I then ask what other entities their organization conducts business with. Many times, one or more of their clients are high-value targets.

Criminals and intelligence services will always evaluate whether a target entity is considered to be hard or soft. The hard target is extremely difficult to penetrate due to robust security protocols. On the contrary, soft targets practically leave the door open with a welcome sign posted at the entrance. When confronted with a hard target, social engineers will identify and carefully analyze whether entities providing products or services to that target might provide the perfect conduit for gaining access. Examples of such service providers for potential exploitation are law firms, CPA firms, staffing companies, IT management providers and other vendors.

The Panama Papers leak revealed the amount of sensitive information that law firms may hold regarding their clients. In this case, more than 2.6 terabytes of data containing 11.5 million files were accessed from a data breach of the world's fourth biggest offshore law firm, Panamanian-based Mossack Fonseca. While the actual identity and methodology used by the source of the breach remains undisclosed, the information was provided in August 2016 to the German newspaper *Süddeutsche Zeitung*. The acquired documentation identified a long list of prominent clients as well as details regarding methodologies used to hide their assets offshore.

Numerous national leaders were on the list, including then Pakistani Prime Minister Nawaz Sharif, ex-interim Prime Minister and former Iraqi Vice President Ayad Allawi, Ukraine President Petro Poroshenko and Iceland Prime Minister Sigmundur Davio Gunnlaugsson. Other accounts were linked to family members or close associates of Egyptian President Hosni Mubarak, British Prime Minister David Cameron and Russian President Vladimir Putin.

While the Panama Papers became a sensationalized breach due to its size and scope of high-profile victims, it also revealed that most law offices likely have sensitive client information that would be of value to threat actors. Such information might reveal details regarding

beneficial ownership of real estate and other assets, merger & acquisition details, negotiation strategies, debt restructuring, litigation planning and more. While successful breaches of law offices are on the rise, most law firms remain complacent towards implementing greater security protocols to better protect information entrusted to them by their clients. This will unlikely change until clients begin to conduct due diligence on law firms and hold them to higher standards.

Say your firm provides engineering consultancy services, and you have many clients, both in the private sector as well as with the U.S. government. You won a bid to provide engineering services for a new state-of-the-art facility being built for a manufacturer of superconductors. That entity is a high-priority target for the foreign intelligence service. Instead of directly trying to penetrate the target entity for collection of proprietary information, the foreign intelligence service would likely try to penetrate your firm to obtain the detailed schematics of the facility. They might even consider recruiting one of your employees with direct unescorted access into the target facility during the project.

Two real-life examples from the retail and healthcare industries also illustrate these risks. In 2013, a security breach at Target compromised payment accounts of about 41 million customers and the personal details of approximately 70 million consumers. Numerous lawsuits were filed against this retailer, and the total costs of the breach exceeded $236 million, including an initial multi-state settlement of $18.5 million to cover state-specific costs associated with their investigations of the breach. Additionally, Target agreed to pay up to $10,000 to consumers who could prove their data was compromised.

How was Target penetrated? It turns out that perpetrators of this attack first breached a third-party HVAC provider based in Pennsylvania. They then stole the computer gateway credentials of this vendor to gain access to Target's network and install malware.

In the 2018 breach of Managed Health Services (MHS), more than 31,000 plan members had their personal information compromised including names, insurance ID numbers, addresses, dates of birth, dates of service and descriptions of medical conditions. While total costs are undisclosed, this breach took a serious toll on MHS' reputation within the health industry.

How did it happen? While attributable to two separate incidents, the first breach was associated with a phishing attack at vendor company LCP Transportation. LCP employees received scam emails, allowing hackers to access their email accounts. Once the perpetrators penetrated the LCP network, they were able to find a gateway into MHS.

Even if you do not believe your organization has anything of significant value to steal, never assume that you are not a potential target. A better posture would be asking whether any of the companies you do business with make attractive targets.

Chapter 2

Collecting Information on a Target Organization

"By failing to prepare, you are preparing to fail."
—Benjamin Franklin

Mounting an attack against a target or adversary is never conducted in a void. All available information is collected in advance and carefully analyzed to come up with the best strategy for maximizing success of the operation while minimizing any potential compromise of equities. Military commanders will diligently collect ground truth before sending in their forces. Terrorists and organized criminal groups looking to kidnap their target will typically mount surveillance for days or weeks in advance to gather information regarding that target's pattern of life. Likewise, professional social engineers who look to penetrate an organization to steal data will definitely conduct their research as well.

As a CIA intelligence officer, I learned to leverage a great internal resource: analysts who provide targeting packages. They collected

information from various public and nonpublic sources, then conducted an analysis and helped better guide my targeting operations. However, at times, I needed to supplement this information with my own research.

Despite a CIA intelligence officer's ability to access nonpublic resources, sometimes the most valuable information is in plain sight. Thanks to the proliferation of the World Wide Web, there are many public resources that appear completely harmless to the average person but present a true vulnerability for a target organization when a social engineer knows how to exploit it.

Organization Websites

My starting point is typically the official website established by the entity from which I want to acquire information. Out of all available public resources, this is the medium the entity has complete control over when it comes to exposing information. While websites back in the late 1990s typically had only a few pages, today's organizational websites can exceed several dozen. They are structured into several categories, each providing tidbits of information of potential value to social engineers.

The "About Us" section will usually outline historical information as well as the entity's mission statement. These details can provide a window into the culture of the organization. What do they value, or what do they want to convey to the public that they value? This can be useful for structuring a pretext or cover story when I eventually decide to approach a member of the target organization. This same section may also identify leadership figures and other key personnel working for the entity. Typically, it will incorporate their pictures, biography and occasionally even contact information.

A "Products and Services" section will detail the commodities the entity is trying to promote. Once again, this information may be useful when developing a pretext for initiating contact with a company representative.

The "Press Releases/News" portion of a website is somewhat useful for identifying recent milestones achieved by the entity or its management. These may include promotions of key personal, contracts obtained, or strategic acquisitions of companies incorporated into the group. Often, such press releases will also include brief statements from key officials.

"Career Opportunities" provide an indication of company growth, whether geographically or in new products or services. Many times, they will also include job postings.

"Contact Us" is a portal through which contact from the outside is solicited—a welcome opportunity for social engineers.

Job Postings

Whether posted on the organization's website or on one of many job-posting sites such as Monster, Indeed, CareerBuilder and Glassdoor, job listings provide a wealth of information. At a bare minimum, listings will usually reveal the basic preferred IT qualifications sought from an applicant, which can provide invaluable insight into the software programs the organization runs on its server.

An example of this was a job posting recently placed on Indeed by a midwestern firm looking to hire an AWS Data Architect. The following details were listed within the job posting under "Technical Requirements."

- Experience implementing AWS Data Services in production Redshift, EMR, EC2, S3, Athena, RDS, DynamoDB, Kinesis, Glue, etc.
- Experience developing distributed data platforms using Spark, Scala, PySpark, Spark-SQL.
- Experience leveraging Big Data Technologies in Hadoop, Hive, HBase, HDFS, Cassandra, Kafka, Sqoop, etc.
- Proficiency in Python, Scala, and/or Java.
- Proficiency in SQL.
- Experience with designing and implementing RDBMS, Oracle, PostgreSQL, MySQL, MS SQL Server, etc.

Prior to the official launch of a new product or service, companies will frequently hire additional employees to support this growth. The job descriptions may provide greater insight into the market focus of the target entity, whether it be growth through current clients, acquisition of new customer accounts or geographic expansion.

With a job posting, a company is inviting contact with someone from the outside, and it provides social engineers an opportunity to submit a resume to HR. Another approach is to carefully choose someone else within the company to forward my resume—and potentially attached malware—to HR. Job postings also provide the ability to interview with the employer, creating an additional opportunity to gather critical information regarding the organization. I could even have one of my team members attempt to obtain employment with the company and become my insider.

Employer Review Sites

Glassdoor has a database containing over 8 million company reviews, leadership and management ratings, salary reports, job interview tips, employee benefits reports and workplace insights all generated by the people who know the company best, the employees. Here, social engineers can gain invaluable insight into what employees like or dislike about working for the target organization. Reviews discussing great opportunities for professional growth,

awesome management, flexible hours and good benefits are just as valuable as ratings that reveal a lack of opportunities for career advancement, antagonistic work environment, incompetent management, long hours or no benefits.

These reviews provide the pulse regarding morale within the organization. Generally, it is much easier to manipulate a disgruntled employee than someone who is very happy and loyal to their employer.

Organization Social Media Sites

While an entity may aggressively use social media to help promote their products and services, an unintended consequence can be the leakage of information, which can be invaluable to social engineers. This exposure results in the creation of vulnerabilities for the organization. Company employees will often upload photos or videos of themselves in the workplace to social media sites, providing social engineers with insight into their physical workspaces.

When hosting events, some organizations will post floor plans. Might they be useful to a criminal wanting to make a physical intrusion? Uploaded pictures will often provide information regarding what actual workspaces look like. Are there offices that might be more difficult to gain access to, or are there open cubicle areas? Or perhaps better still, are there shared lounge areas where employees can just take a seat, resulting in less scrutiny over who really belongs in the area?

Gaining an understanding of employee dress code can be useful if I am sending someone inside and want them to fit in. In addition to dress, pictures frequently reveal information regarding the types of badges used by the company and how employees display them. If I know the specific design of the badge, one can easily be manufactured for flash purposes.

Occasionally, shared pictures will capture the names of posted WIFI networks or passwords. Photos taken in front of employee workstations will frequently provide detailed information regarding the brand and model of computer hardware. If the screen is left turned on, I can see what browsers and specific software programs are used within the organization. Sometimes these photos may even show emails or documents left on the screen.

Creative Google Searches

When looking up a topic on Google, most people will only view up to the first 12 entries. However, there are easily thousands of entries regarding large companies, and some of the most interesting information for social engineers is found well beyond the first page of results. For this reason, conducting creative searches is crucial. A simple search of the company name and “pdf” may surface employee

manuals, employee benefit packages, IT user guides, executed nondisclosure agreements and other documents containing sensitive information. The different companies that are subcontracted by the target company for services such as janitorial, trash disposal, catering or temporary staff can often be identified within such documents—a key resource for exploiting contracted service providers to breach security.

The Wayback Machine

A common misconception regarding the internet is that once an organization has deleted or modified information previously contained on its corporate website, the original information is no longer available to the public. Fortunately for social engineers, this is not the case. The Wayback Machine (www.archive.org/web) is a digital archive of the World Wide Web. This free resource enables users to see archived versions of web pages across time, as far back as 1996. Therefore, even if the target organization's new security director decided that some of the information on a company's website should be removed, the Wayback Machine can be used to potentially retrieve it.

Reconnaissance Made Easy

I do not have to physically walk the street to see what the target's office building looks like—I can do it virtually through maps and satellite imagery offered by Google Maps and Google Earth, which provide images of the target's office building and even an individual's residence. If I wanted to launch an intrusion into a target office, I would want to learn as much as possible about access points. For example: Are there guards? Are they armed? Is there video surveillance? More importantly, I would want to find out what businesses are near the target location such as coffee shops, bars, restaurants, fitness centers and office supply stores.

This type of intelligence is important because it helps me identify places where individuals from the target facility might hang out during the workweek, providing opportunities to casually bump into them. That could result in a conversation where I can carefully elicit information. Alternatively, it could lead to an opportunity to develop an employee for use as a future insider source. Other afforded opportunities may be the theft of the employee's credential, facilitating an intrusion into the target's building or the theft of the employee's laptop, which likely contains proprietary information.

Additionally, I can use geographical information in order to identify locations in the vicinity that make deliveries to the target's office, such as flower shops, restaurants or office supplies. With this information in hand, I may decide to impersonate someone making a delivery to obtain unescorted access onto the premises.

Identification of Employees

The internet can be exploited to identify the names of many target organization employees as well as their positions. By far the most resourceful site used by social engineers for this purpose is LinkedIn—an estimated 40 percent of a firm's employees have their own LinkedIn profile. Other resources for identifying employees include the organization's official website and social media pages. The identification of employees is a crucial step for social engineers in planning their attacks.

Additional Online Resources

While there are many fee-based subscription services that provide information on corporate, nonprofit, academic and government organizations, the following list identifies sites that provide useful information for free:

Bloomberg – news stories on companies as well as related financial data

www.bloomberg.com

Corporate Information – free and subscription-based information for companies across all countries

www.corporateinformation.com

Directory of Associations – list of all local, state, national and international professional associations and chambers of commerce

www.directoryofassociations.com

Dun & Bradstreet – frequently updated information on worldwide companies; free as well as fee-based services

www.dnb.com

Education Corner – lists over 7,000 colleges and universities across the U.S., providing their profile and associated links

www.educationcorner.com/colleges-universities.html

GuideStar – the world's largest information resource on nonprofit organizations

www.guidestar.org **Opencorporates** – the largest open database of companies in the world

www.opencorporates.com

Privco.com – predominantly fee based and focused on private companies

www.privco.com

U.S. federal government – links to all federal government departments and agencies

www.usa.gov/federal-agencies

U.S. municipalities - indentification of state-by-state municipalities and links to their websites

www.en.wikipedia.org/wiki/
Category:Lists_of_towns_in_the_United_States

U.S. Secretary of State websites – very useful for researching companies incorporated within a specific state

www.thebalancesmb.com/secretary-of-state-websites-1201005

U.S. Securities and Exchange Commission (SEC) – information on all publicly held corporations, including public filings

www.sec.gov

U.S. state governments – links to state government programs and offices

www.usa.gov/states-and-territories

Chapter 3

Selecting Insiders and Collecting Personal Assessment Data

> “A lot of hacking is playing with other people,you know, getting them to do strange things.”
>
> — Steve Wozniak

Gathering information about organizations is one thing, but selecting, assessing and manipulating individuals within those organizations takes a different approach. In general terms, an insider is anyone who has regular unescorted access into the target organization, whether the physical premises or the organization’s IT network. This includes all employees from the receptionist up to the CEO. In addition to employees, contractors and outsourced services such as security guards, food caterers, cleaning and trash disposal personnel and IT technicians could become insiders. These contracted service providers could likely be identified through creative Google searches.

Not all potential insiders need to be considered— a small pool of well-placed individuals on whom I can collect useful assessment data is sufficient. For example, if an organization has 300 employees, chances are that they have five to ten potential inside targets worth my consideration. Learning about their areas of responsibility will help appraise their direct or indirect access to the information I seek. Upon validation of their likely access, I will then want to learn as much as possible about them to develop a personality profile assessment. This assessment, which will include identified motivations and vulnerabilities, will be key to structuring a plan to effectively manipulate them.

Prior to the abundance of resources available on the internet, intelligence officers initially targeted potential insiders with little information beyond their name and organizational title. I could only speculate on their potential access and had no personality profile prior to approaching them. It was only after a series of face-to-face encounters that I was able to determine their access and obtain invaluable assessment information on them. This process would take several months to accomplish, and in some cases the intended target ultimately did not have the desired access or lacked personality characteristics that would make them suitable for manipulation. I would then drop them and move onto another potential insider— options were very limited.

Today, the internet provides intelligence officers and criminals alike with a tremendous amount of resources to accomplish this task

with greater efficiency and total anonymity. While it is commonplace and expected for organizations to have public information easily searchable online, finding intimate details about individuals can be more difficult. However, social media profiles have become key for intelligence gathering on otherwise private individuals. Hidden in plain sight, the following aspects of popular social media can provide a surprising amount of information.

LinkedIn

Profile photo – using Google images or tineye.com, I can identify other locations on the internet where this picture may exist.

Heading – indicates how the target wants to market themselves within the LinkedIn community.

Academic History – identifies degrees obtained or in progress. Individuals typically have a strong affinity to their alma mater, which can be leveraged when making an approach.

Employment History – helps me understand their career progression and goals while providing a detailed description of their responsibilities at the target organization, which gives clues to their potential access. Occasionally, this section may also detail former employment with a target organization where the individual may still maintain relationships, facilitating indirect access.

Certifications and Licenses – identifies professional organizations where they likely maintain memberships.

Publications – reveals areas of professional interest and expertise; provides topics that can be discussed with the target during initial contact.

Postings – reveals people and issues of importance to them. Often the individuals who post "likes" to a target's post have a closer relationship to the target compared to most identified connections.

Volunteering – identifies causes that they are passionate about.

Influencers – identifies people and qualities they would like to emulate.

Connections – reveals how open or closed (reserved) they may be to someone approaching them. Identified connections can be used as referrals to the target, or the target can be used to make a referral to another target of interest.

Facebook

Profile Description – often includes birthday or actual date of birth, current and previous cities where they have lived, current or previously attended universities, memberships in social organizations, relationship status and favorite sports teams, movies, books, music genres and artists.

Pictures - these include pictures of the target insider in a variety of

social interactions, photos of the target's family and friends and the identification of their network of contacts whose Facebook pages can also be exploited. Such photos frequently reveal socioeconomic status, material desires, hobbies and favorite pastimes, favorite foods and restaurants as well as locations of past travel.

Posts – the same information can be gleaned as in pictures, but posts also include details regarding events of importance to the target. Frequently a target will reveal plans such as upcoming travel and attendance at events. Through pictures and postings, parents may easily reveal sensitive information regarding their children including names, ages and identification of their schools.

Sometimes people challenge me by stating, "Most people use privacy settings!" Really? Based upon my experience, I have found that most people don't maximize the use of privacy settings. Besides, even if a target is using privacy settings, I next check their spouse or children's accounts—there is always someone who doesn't have strong privacy settings.

Twitter

Just like that little blue bird in the logo, targets often love to tweet. They give us a play-by-play action of where they are, what they are doing at that moment and even what they are thinking. In addition to their own comments, who they decide to follow can also provide insight into their interests and opinions. Twitter profiles can reveal information regarding political leanings, ideology, religious convictions and things that please as well as irritate them—that's pretty revealing.

YouTube

Owned by Google, YouTube is the largest repository of videos available on the internet. In addition to searching for topics of interest, many people will upload their own videos or establish their own channels. These channels are useful for identifying topics of interest to the channel owner and can provide additional insight. When producing their own content, these videos will often reveal information about their home or offices.

Instagram

Owned by Facebook, Instagram has become one of the most popular social networks for the sharing of photos and short videos and is another source for intimate details about a target's daily life, inner circle and interests.

Pinterest

Pinterest has grown to be one of the most important social media sites focusing on visual content. Whether posted as a hobby or for work, the photos and links a target saves can provide insights into their passions as well as business interests.

Tumblr

Tumblr is a popular social blogging platform predominantly used by teens and young adults. It will reveal topics of interest to a target as well as the extent of their knowledge or bias on issues.

Medium

As opposed to Tumblr, Medium is a social blogging platform used predominantly by adults who are readers and writers.

Flickr

An image and video hosting service, as well as an online community, popular among amateur and professional photographers.

Reddit

This social media site is an extremely popular platform for people to ask questions, post comments and share links to videos, photos and other content relevant to the subject.

Tinder and other dating apps

This is a very popular location-based dating app that matches people located within a particular area. Users can set up a brief profile highlighting their photo, bio and links to social media accounts, allowing anyone matched up to them to anonymously learn more.

PeekYou

While not a social media platform, PeekYou collects scattered content from social media, homepages, blog platforms and news sources to present online identities. It is very useful when trying to identify all of the social media sites used by a target.

TinEye

TinEye and Google Images are two great tools that can identify other locations where the same photo might be found on the internet. Just like PeekYou, it is a tool to identify other social media sites used by a target.

I often compare searching through social media to dumpster diving. In the investigative world, dumpster diving refers to physically going through someone's trash at home or at work to collect clues or evidence. Criminals also do it. What could someone learn about you if they went through your trash? Imagine dumping the contents of your trash onto a table—you would be amazed about how this trash may reveal where you buy your groceries, where you get your takeout from, what your food preferences are, what charities you receive correspondence from or what magazines and newspapers you subscribe to. It may also include actual bank statements, or at least discarded envelopes, which will help identify the financial institutions you have a relationship with. Those discarded pill containers will identify which prescription medications you are taking along with the dosage amounts, the name of your pharmacy and occasionally the name of your doctor. That's a lot of exploitable information.

Like the items that can be discovered dumpster diving, there is a lot of extra and unnecessary information that people frequently place on social media. Social engineers do not always know why the target wants to push all of this information out for public consumption—perhaps it's for social acceptance, vanity or competition. However, social engineers do not care why—they just happily exploit it.

Using Appendix A, *Personal Assessment Questionnaire*, I encourage the reader to review their own social media profiles to ascertain whether posted information makes them potentially vulnerable to a social engineer.

◆◆◆

With the information gleaned from social media profiles, social engineers can now formulate a personality profile assessment, which focuses on motivations and vulnerabilities that can be leveraged for the ultimate manipulation of the target.

Motivations are those things that people are passionate about—things that get people out of bed in the morning to start our day. Examples include the following:

- Money (accumulating money as well as what money can buy)
- Family (the welfare of parents, siblings, children)
- Education (for themselves as well as their children)
- Career (progressing in one's career)
- Better home (larger, nicer, better neighborhood)
- Luxury goods (sports cars, artwork, jewelry, other status symbols)
- Desires/wants (dreams of travel, having their own business)
- Altruism (volunteering for a cause, philanthropy, mentoring, coaching)
- Ideology (capitalism, socialism, communism, extremism)
- Religion (strong faith convictions)
- Politics (conservative, liberal, political party supporter)

While motivations are considered positive factors, vulnerabilities are usually considered weaknesses. However, they can also be leveraged by a social engineer when manipulating their target. These may include:

- Money (extreme financial hardship)
- Gambling (addiction to physical or online gaming leading to financial hardship)
- Drinking to excess (leads to family/social problems, health issues, lowers barriers to elicitation of information)
- Drug addiction (strong chemical dependency to illegal or

controlled substances)

- ➢ Sex (can be easily baited, lend themselves to extortion or blackmail)
- ➢ Greed (they can never accumulate enough power or wealth)
- ➢ Revenge (desire to get back at someone like their supervisor or organization)
- ➢ Hate (usually linked to revenge)
- ➢ Jealousy (coveting something that someone else has, wanting to do better than them)
- ➢ Guilt (over something they did or failed to do in the past)
- ➢ Ego (wanting to constantly prove their intelligence and capabilities)
- ➢ Low self-esteem (looking to someone who can help lift them up)

By far, one of the most prevalent vulnerabilities is financial. At the time of this writing, the COVID-19 pandemic has resulted in severe financial stress for many people on a global scale. While the target may have retained their job, perhaps another member of the same household has lost their income. Lost revenue can be very disruptive, leading to tensions and problems in relationships. It can also drive people toward some of the previously identified vulnerabilities such as gambling, drinking, drug use or extramarital affairs.

Several intelligence services, including the Russians, Chinese and North Koreans, are known to leverage vulnerabilities when trying to manipulate targets. They will frequently orchestrate events that lead to a seriously compromising situation for the target. These may include extramarital affairs with photographic evidence used to extort the target, or the breaking of some local law that could result in incarceration. In such cases, the target is offered an opportunity to avoid these consequences in exchange for their cooperation. While this may be a successful ploy for a short-term operation, it does not leverage trust, only fear and resentment.

I found in my career as a CIA officer that leveraging motivations, rather than vulnerabilities, was much more effective. Targets were more receptive when they perceived personal benefit from cooperation. Typically, when targets displayed significant vulnerabilities, such as excessive womanizing, heavy drinking, drug addictions or severe financial problems, these vulnerabilities were hard to control and could lead to serious security problems.

I once recruited an individual who would become instrumental in the design and execution of a high-profile operation. His cooperation was predominantly leveraged by severe financial duress. With carefully measured financial assistance, he got back on his feet and

was able to move our operational objectives forward with incredible success. However, he had other vulnerabilities, including excessive drinking and severe womanizing. On one occasion while intoxicated, he crashed and totaled his car, and I had to help him procure a replacement. During another drinking binge, I lost complete contact with him. He reappeared only moments before his participation in the next crucial phase of the operation, claiming to have lost his wallet and cell phone to a group of robbers. While ultimately a very successful operation, the source's vulnerabilities posed security risks to the operation and really tested my patience.

Once a social engineer has developed a personality profile for their target—taking into special account motivations and vulnerabilities—it's time to make contact.

Chapter 4

Designing a Pretext for an Approach

"A con artist's only weapon is his brain."

—Frank W. Abagnale, *Catch Me If you can*

Once a social engineer has gathered all available useful data on the target organization and identified plausible insiders, they need to develop the pretext or cover story for an approach. This pretext needs to be logical as well as attractive enough to get the insider's attention. As successful sales professionals know, it is all about identifying the prospective customer's pain and then offering a potential solution to their problem. If the approach does not appear to benefit them in any way, they typically will not welcome it.

Conceptually designing that pretext and then executing the entire plan was what I most enjoyed during my career with the CIA. It required careful study of the target, creativity in the formulation of the approach, use of a variety of interpersonal skills, extreme flexibility and continuous adaptability. Most of all, such operations energized me and frequently gave me an adrenaline rush.

Just as criminals will not introduce themselves as professional fraudsters to their targets, intelligence officers will not reveal their true affiliation. As a result, it is crucial that the pretext for the initial approach has nothing to do with intelligence gathering. Over the course of my career as an intelligence officer, I assumed multiple identities and portrayed various professions. Depending upon the circumstances, I could also pretend to be another nationality than American. This required modifying my accent in English or the use of three foreign languages I am familiar with.

Crucial to the success of a pretext is some degree of cover backstopping, or creation of the backstory. No matter how strong the backstopping, successful intelligence officers must fit the profile of the persona they intend to portray. If they do not, their cover will quickly be compromised. A common saying during our training was, "If you pretend to be a duck, you can't act like a turkey. You have to walk, swim and quack like a duck."

The general public's perception of working undercover is typically

warped by Hollywood. Films often show law enforcement officers who infiltrate drug rings or other criminal networks for the purpose of bringing them down. As part of their cover, the officers flash a lot of cash, wear expensive clothing and drive sports cars containing an arsenal of weapons in the trunk. They easily slip back and forth from being undercover for specific meetings to returning to their normal lives.

For an intelligence officer, going undercover is no short-term glamourous adventure. It takes years of training followed by years of practical experience and seasoning. Initial training focuses on spy tradecraft—how to conduct clandestine operations without discovery. However, equally important, if not more so, is the officer's ability to understand operational requirements and how to best design and develop their cover to effectively insert themselves into circles of individuals who can help satisfy intelligence collection requirements. To be accepted and trusted by such individuals, intelligence officers cannot display any characteristics that would arouse the suspicion that they are not who they claim to be.

An intelligence officer must also adhere to the norms for individuals that work in the profession they are emulating. In addition to maintaining an appropriate economic status, they must include a credible legend regarding the progression of their career and their competency on topics within the field. The slightest discrepancy can draw suspicion.

The danger for some officers is the complacent belief that if they have not been seriously challenged regarding their story, it must be working. In many cases, people who might suspect that something is strange about the individual will not directly confront them. However, they will talk amongst themselves, which could eventually lead to the filing of a report with local authorities. Once the local jurisdiction has taken an active interest in the activities of the intelligence officer, the house of cards may quickly come tumbling down.

While during my career my activities were never seriously challenged, I did learn of colleagues working overseas who were compromised. Several of them were briefly detained by authorities and then expelled from the country as persona non grata. Others were imprisoned and deprived of their liberties for extended periods of time. Over the course of the history of the CIA, there have been many officers who died in service to their country. Inside the entrance to CIA headquarters is a memorial wall that contains rows of stars. The inscription above the stars reads, *"In honor of those members of the Central Intelligence Agency who gave their lives in the service of their country."* As documented in *The Book of Honor* by Ted Gup, several of those stars are attributed to undercover intelligence officers who died

in action or while serving life sentences in foreign prisons.

Intelligence offers are typically required to live their cover 24 hours per day over extended months, if not years. Perhaps the biggest challenge of this lifestyle is loneliness. While living in a sea of people, many of whom could be considered close friends and acquaintances, the officer is never allowed to be transparent. They will always have to conceal who they really are. This creates difficulties in developing intimate relationships and can serve as a true barrier to marriage. Those fortunate enough to establish a family will also place the burden of secrecy upon their loved ones. Many times, the stress of the job and managing the web of lies can literally tear couples and families apart.

The Russian Illegals Program is a prime example of how extreme the development of cover can be. Run by the Russian Foreign Intelligence Service (known by its Russian abbreviation, SVR), candidates are selected and isolated at a very young age for preparation to become immersed into a specific foreign country and assume the identity of a citizen of that chosen country. They receive extensive training regarding the history, culture and traditions of their future "homeland," as well as subtleties in the local language. While these illegals have been known to operate in several countries, the most notable recent example came to light in the United States with the June 27, 2010 arrest by the FBI of ten Russian illegal agents. Among them was Ana Chapman, who gained the most attention from the press due to her femme fatal attributes. Shortly after the arrests, the agents were part of a prisoner exchange between Russia and the U.S.

Probably one of the best Hollywood-generated depictions of illegal agents is the series *The Americans*. While this six-season drama accurately reflects many of the challenges faced by illegals, the portrayed operational tempo during a 24- to 48-hour period far exceeds what most intelligence officers would face over the course of several weeks, if not months.

◆◆◆

In reality, most threat actors will not invest in the time and effort to develop the same depth of cover sought by true intelligence professionals. However, there are still a number of factors they will need to consider when designing their strategy to ensure that their cover pretext will assist them in gaining access to their target while defending against any cursory due diligence resulting from curiosity or suspicion.

This process can be illustrated by a criminal group's interest in

breaching the security of a large South Florida wealth management company, Petra Wealth Group (PWG). Let's say the criminal enterprise seeks to uncover the identities of PWG's top high net worth clients. In addition to their names, the criminals would likely seek additional sensitive information including their personal family details, business holdings, financial transactions and account information. Such information could be sold on the dark web or to directly target one or more clients.

The criminal group would first attempt to identify who within PWG might have access to such information. While their initial internal discussions focused on targeting someone within PWG's IT department, they soon realized that such an insider would likely not have access to anything more than transactional data such as account numbers, account balances and wire transfers. This approach would not surface the names of individuals who were the account holders, nor any specific information regarding their personal lives or business dealings. It was finally concluded that such details are only known by PWG's account managers, who maintain a separate file on each client detailing the history of the account. While specific individuals may be assigned to maintain the relationship with their own clients, such information must remain accessible to other account managers in the event they need to service the customer in the absence of the assigned account manager. Furthermore, these account managers will also have access to many of the same transactional reports that are automatically generated by the IT department.

Now that the category of target insider has been identified, the criminal group will attempt to identify several candidates. They learn that PWG has six full-time account managers. Out of these six, the group has been able to obtain substantial information on four of them through the review of their social media profiles, along with other internet research.

They identify Javier Acosta as a very attractive candidate. He joined the firm three years ago after having obtained his master's degree in business administration from a local university. He appears to be very career driven, having been promoted from an assistant account manager to a senior account manager in the span of 18 months. He had also authored several short articles on LinkedIn, including one stating that wealth managers need to take better advantage of technological tools to enhance customer service.

The criminal group ultimately decides to attempt to approach Javier. They plan to offer a trial version of a new software program said to enhance an account manager's ability to identify significant life-changing events of clients such as marriages, births of children and deaths of close family members as well as professional milestones

such as promotions or awards received. In addition to highlighting events that would prompt the account manager to reach out and offer a congratulatory message, it would provide recommendations for the marketing of additional products and services related to the event. Additionally, the software would also help identify individuals closely linked to the client by familiar, social or business ties, offering considerable potential for surfacing strong market leads that could leverage potential referrals from current clients.

The criminal group chooses team member Gary Johnson for this direct approach due to his background in software development. To decrease blowback to Gary in the event of a compromise, they decide that he would develop and use an alias persona for this specific requirement.

In preparation for this assignment, Gary needs to develop and memorize his personal alias legend. He comes up with the following:

Name: Gary Sutherman
Born: 18 November 1976, Chicago, Illinois
Civil Status: Single
Parents: John Sutherman and Cynthia (Prado) Sutherman
Siblings: One younger brother named Matt
University Studies: BS in Liberal Arts and MBA from University of Illinois at Champagne – Urbana
Past Employers: Names of two large multinational firms
Current Employer: Los Angeles-based Quest Innovative Solutions, LLC
Position: Business Development
Current Residential Address: Montclair Brentwood Apartments, 11965 Montana Ave, Unit 57, Los Angeles, CA 90049A

Gary decides to use his first true name, a common practice given that there is always the possibility of running into someone who knows him. All the additional information is made up and relatively easy for Gary to remember and defend. By claiming to have studied and worked at very large organizations, he made it extremely difficult for anyone to verify. Using Google Earth, he virtually toured the areas around the University of Illinois and his ostensible residence in Los Angeles for basic familiarity in the event he ran into someone who was familiar with these areas. With the exception of his current employer's identity of Quest, he felt comfortable in defending this basic level of cover without any need of backstopping.

Gary spent approximately 10 hours building a basic website in the name of Quest. He set up a functioning business email address and paid cash for a non-attributable prepaid cell phone with an area code from the greater Los Angeles metropolitan area. He contracted with a local business center to establish a virtual office for his company,

providing Gary with a business address and associated telephone number. Receptionists working at the center answer calls to the assigned number in the name of Gary's company and offer to take messages for him.

With the basic structure in place, Gary must now undertake a more laborious task. He will need to develop a robust working knowledge of the wealth management industry, along with the services they provide to their clients. It is paramount that he appears legitimate during his initial encounter with the target, which requires his use of industry terminology and a high level of confidence. Gary is a quick study and can procure most of this industry background via research on the internet. Time permitting, he might even try to attend an industry event to obtain a sense of how industry professionals conduct themselves—he would like to emulate Javier as much as possible.

If Javier is comfortable with this first encounter, the unsuspecting target will likely do little more than conduct a cursory review of Quest's website. If Javier wants to dig one level deeper, he might try calling Gary's company, and would feel reassured when the call is answered in the name of the company by the receptionist working for the business service center.

Once fully prepared, Gary looks for a way to connect with Javier. Instead of trying to place a cold marketing call, which risks a turndown, Gary attempts to casually run into his target during the monthly chapter meeting of the Private Wealth Management Association (PWMA). Gary has noted that Javier is the current treasurer for the chapter and assumes he regularly attends. As the chapter is always interested in potential new members, Gary would claim that a west coast PWMA member recommended that he consider visiting a future event. Ironically, the chapter meeting Gary plans to attend features a guest speaker on the topic of protecting wealth from fraud.

After the speaker gives her presentation and near the end of the meeting, Gary approaches and strikes up a conversation with Javier. They speak for about 15 minutes, then Gary offers to take Javier out for lunch the following day. He wants to explain some of the software products his firm is attempting to market within the industry and would greatly appreciate Javier's insight. As the concept hits deep in the heart of Javier's desire to incorporate such technological tools, he readily accepts.

During the lunch meeting, Gary builds very strong personal and professional rapport with Javier and explains how several prospective clients in the industry are in the process of procuring his organization's software products. Javier expresses strong interest but

advises that any such product would require a full review by his company's IT department before a decision could be made. He asks Gary if a demo could be arranged. Gary readily suggests an intermediate option—he could give Javier a thumb drive containing a 10-day limited trial for a single user. Javier could install it on his own terminal and import data for up to three clients. This software would fully integrate with the internet browser used by the firm, and he would be able to see the results for himself. If Javier is satisfied and believes that his firm could benefit from such a tool, Gary could then arrange for a demo while Javier would obtain the support of key officials in his company for making the purchase.

Javier enthusiastically takes the thumb drive and inserts it into his office computer within minutes of arriving back to work. While the program appears to be loading, it consistently stalls in the middle of the installation. A disappointed Javier will later telephone Gary and leave a message on his cell phone, and in the coming days will feel surprised and puzzled that Gary never returns his call. Within three days of the attempted installation, Gary's criminal group will extract 1.3 terabytes of data from Javier's employer.

Chapter 5

Leveraging Psychology for Manipulation: Trust and Influence Factors

"Trust is like blood pressure. It's silent, vital to goo health, and if abused it can be deadly""

—Frank Sonnenberg, author of Follow Your Conscience

"When it comes to controlling human beings, there is no better instrument than lies. Because you see, humans live by beliefs. And beliefs can be manipulated."

—Michael Ende

Social engineering, by definition, is the ability to manipulate another human to undertake an action that may not be to their benefit but will serve to accomplish the objectives of the social engineer. As noted in previous chapters, collecting information on the targeted individual will help determine which motivations or vulnerabilities particular to that individual can be leveraged in the approach. Social engineers also take advantage of additional psychological factors that make most people susceptible to manipulation.

Trust

The concept of trust is extremely powerful. Trust has existed since the dawn of civilization and serves to bring people together to form societies. Even the early cavemen formed small groups of people who trusted in one another for the purpose of survival. Trusting in others is considered crucial for people's wellbeing—without it, humanity would see the breakdown of world order and utter chaos. However, the main character trait that makes humans very vulnerable to social engineering techniques is the tendency to blindly trust everyone, even people they do not know. As I was quick to discover in my career, this is especially true in American culture.

Like many Americans, I was brought up by my parents to trust everyone, until a person gave me a reason not to. Unfortunately, I had

to go through several painful experiences to realize that I needed to better temper my trust. Many of these lessons were taught early in my business career during interactions with international executives. On the surface, they appeared as friendly and genuine as anyone else. Later, after I got burned, I learned that some people in other cultures only trust those within their inner circle, including family members and close friends. Anyone else was fair game to take advantage of, and this was considered perfectly normal.

While trust is often influenced by regional and cultural factors, Americans need look no further than their own history to identify several famous fraudsters who successfully preyed upon their victims' trust to swindle massive amounts of money. One recent notorious case was Bernie Madoff. He convinced more than 4,800 wealthy individuals to entrust their money in his investment Ponzi scheme, and ultimately defrauded them of approximately $65 billion until his arrest in 2008. This scheme was originally named after Charles Ponzi, who infamously bilked investors out of more than $20 million in the early 1900s. One of my favorite fraudster stories is that of Charles Parker, who successfully got investors to buy several famous landmarks from him, including the Brooklyn Bridge. Parker's scheme was the origin of the expression "If you believe that, I have a bridge to sell you!"

As an intelligence officer, I found that garnering and building trust was exceptionally easy for me. When initiating contact, I would try to leverage the preestablished trust that the target likely had in the individual or entity I was associating myself with. Whether true or contrived, I would frequently say that this trusted person or organization highly recommended that I speak with the target—as salespeople know, referrals are very powerful. Even if the target perceives no personal benefit in meeting with you, they will frequently accommodate the request in order not to burn any bridges with whoever recommended them.

A few specific examples illustrate how a social engineer can structure and deliver a referral that appears to come from the Association of Cyber Intelligence Professionals (ACIP) to their member, Susan Catherwood, Chief of Operations at Dynamic Winds, LLC.

- Place a call to ACIP and ask if they can provide contact information regarding one of their members you are interested in potentially contracting. You believe the company's name is Dynamic Winds. The association would likely be able and willing to provide such information, as they exist to serve and promote their members' businesses.
- Telephone Susan Catherwood and comment that during a

recent conversation with ACIP President Doug Frey, he mentioned the name of her company.

- ➢ Telephone Susan Catherwood and comment that she was recommended by the secretary of ACIP.
- ➢ Call Susan Catherwood and comment that your online research regarding the industry indicated that she was highly recommended as an expert in her field. In fact, her name even surfaced several months ago when speaking with an (unidentified) member of ACIP.

While none of these referrals are genuine, they would likely be accepted and facilitate a conversation with Susan. Unless she became very suspicious of the social engineer's demeanor or proposition, Susan is unlikely to attempt to verify the referral. She automatically trusts the social engineer's explanation regarding the source of the referral.

As previously mentioned in Chapter 2, social engineers will always identify the universities from which potential targets have graduated. Many people feel a strong bond with their alma mater, and it can be a great ploy for initiating contact.

Leveraging well-formulated pretexts or referrals from trusted parties is great for obtaining the initial meeting with a target. After that, the social engineer must use their interpersonal skills to build additional trust. Once in the target's presence, it was always important for me to greet them with a firm handshake, a warm smile and periodic direct eye contact. I needed to connect on a human level, quickly learning about what was important to them and then relating a personal anecdote, whether genuine or contrived, that would serve to create a common bond and lead to rapport. I found incorporating humor was always beneficial as it served to put them at ease and lower their guard. Being able to speak in their native language and discuss current events of interest was always an added plus.

While I spent considerable time preparing and rehearsing my cover pretext in advance of an initial encounter, it was never foolproof. That said, I was amazed at how frequently people would dismiss something that may have surfaced during our interaction that could have called into question my legitimacy. Perhaps it was a lack of knowledge in specific industry terminology or an inability to adequately address a question posed. While it might appear strange to the target when it occurs, they frequently rationalize it as only a minor inkling that something is not quite right. Ultimately, they want to trust you and will do everything they can to justify it.

Social engineers use a variety of techniques to exploit their victims' trust and pretend to be someone other than themselves. Without trying to verify, these victims readily accept what they see,

read and hear. Only afterwards do they lament that they were so easily deceived. Unfortunately, the price to pay for that lesson is typically millions of dollars in financial losses for their organization, or their own personal financial ruin.

◆◆◆

Trust almost always lays the groundwork for a successful interaction with a targeted individual. But in addition to leveraging trust, professional social engineers will also use the following influence techniques.

Liking

As victims are more likely to provide assistance to someone they find to be pleasant, the social engineer will attempt to develop strong personal rapport prior to making the request. This approach can begin during the initial interaction by being very pleasant, maintaining eye contact, smiling and perhaps demonstrating that they have something in common, which helps form a bond. For example, if I have seen on the individual's social media profile or a diploma displayed in their workspace that they went to the University of Wisconsin, I can pretend to have visited Wisconsin. I can easily discuss having experienced extreme cold, going to a Green Bay Packers game or enjoying beer and brats. I immediately develop a bond with this person.

Authority

Victims are more likely to comply if they believe that the request is coming from someone in authority or representing authority figures such as the boss, building security or law enforcement. People tend to not question the request or whether it is rational—they feel an obligation to immediately comply, especially if they believe that failure to comply may result in negative consequences for them. For example, if approached by someone dressed in a security uniform, most people would not question the legitimacy of instructions given to them.

Reciprocation

After the social engineer has conducted a small or low-stakes kind deed for the target, the latter will often automatically reciprocate by performing a similar kind deed for the social engineer. A very basic example is holding open the first set of double doors for someone coming behind you. Almost certainly, that person will walk through and then hold open the second set of doors for you to pass through.

Obligation

Victims will often feel a strong sense of obligation to help the

social engineer after having a significant courtesy or favor extended to them. Examples of this could include the social engineer helping the individual with a problem and then subsequently asking them for a favor. Other examples may be a sense of obligation felt after having been taken out to lunch by, or receiving a gift from, the social engineer.

Concession

Here the social engineer will ask for something that the victim initially finds implausible to comply with. The victim will subsequently agree to comply with a request from the social engineer that appears to be meeting halfway. This type of interaction can be as straightforward as the following example:

Receptionist: Sir, you must have an appointment for authorization to proceed to the executive floor.

Social engineer: I understand. I will come back after setting one up. However, I previously spoke with Mr. Grim and mentioned that I would be sending product information to his attention. I understand that he will be leaving on extended travel later today. I really need to get this information to him. Can I just drop this off with his executive assistant? I will be in and out in less than five minutes. You can even retain my driver's license if you would like.

Receptionist: Okay, no problem. You can leave your driver's license with me.

Scarcity

The social engineer can put pressure on the victim to make a quick decision as the window of opportunity for the victim is about to close. This tactic is frequently used in sales gimmicks such as "while supplies last," "going fast" or "only two more left." As a result, the target makes the decision without an opportunity to obtain further information for proper evaluation.

Consensus or Social Proof

The social engineer may place pressure upon the target by implying that refusing to assist will be seen by others as socially unacceptable. Many of us have personally experienced this at a checkout counter when the cashier asks aloud, in the presence of other customers, whether we want to contribute to a particular charity. You feel like everyone is waiting to hear your response, and you might feel greater pressure to contribute compared to having received a similar solicitation through the mail.

These influence techniques can be used in a variety of situations, including brief one-time interactions with a target.

Chapter 6

The Art of Elicitation

"Everything you say should be true, but not everything true should be said."

—Voltaire

"The wise person has long ears and a short tongue."

—Proverb

There are typically three different ways to extract information from people that are used in very different situations. The first is interrogation—asking direct questions of the detained interrogee to extract critical information. This is typically considered a very hostile approach to information extraction and may include the use of torture or sleep deprivation.

The second method is referred to as an interview or debrief. The individual posing the questions is in a position of authority and asks specific questions of the interviewee regarding a specific topic. This could be an interview conducted by the director of security of various employees following a security breach. It could be a debrief of an intelligence source by his case officer. It could be an interview by HR of a candidate interested in filling a new position. In such situations, the interviewee is not detained and completely understands the context of the questioning.

The third method, called elicitation, is the acquisition of information from a person while not disclosing the real intent of the interview or casual conversation. Elicitation is one of the most important tools used by social engineers attempting to breach security because they can control the conversation and get the target to talk while effectively listening. The social engineer can elicit information whether they're bumping into a target at his favorite local café, sitting next to her on the airplane or targeting him at an industry trade show.

Elicitation is not only conducted during face-to-face encounters, it is also used by social engineers in various online communication platforms as well as by phone.

As an intelligence officer, I received extensive training in elicitation techniques that I used throughout my CIA career. What information was I after? The same information that other intelligence officers and criminals tend to seek—it might be information regarding the target organization that is not readily available and would help me get closer to my objective of breaching their security. It might be the identification of key insiders in the organization who have access to the information I wanted to steal, or it might be information that helped me understand the security vulnerabilities of that organization's operations. In many cases, it included specific confidential or proprietary information that officials were not authorized to disclose.

There are several successful elicitation techniques I used most often in my career. Keep in mind that anyone could have these approaches used against them—especially if they are approached by someone who they do not already have a relationship with.

Closed versus Open Questioning

Closed questions are those which typically seek a very short response, such as a "yes" or "no."

Elicitor: Does your current position require you to travel overseas?

Target: Yes, I travel periodically for my job.

Open questions are asked in such a way to elicit responses that will go beyond a few short words. They will require the target to go into detail.

Elicitor: What would you say are your favorite and least favorite overseas places that you have had to travel for your job?

Target: My favorite is travel to Turkey. I love the food and the Turkish people. It also allows me to practice my Turkish. My least favorite are trips to China. It takes so much longer to get there. Unfortunately, I don't speak any Chinese and I really have not had any opportunity to sightsee. I spend all my time in meetings or at the hotel.

Flattery

Everyone loves to be complimented, whether on their clothing, appearance, professional success or family.

Elicitor: Wow, you appear to have progressed very well in your position and could serve as a great inspiration for those just getting started in this profession. What would you say were your main keys to success?

Target: Oh, you are so kind. I would like to attribute it all to my own efforts. However, I was very lucky to work several years under the tutelage of Mr. Brian Williams before he moved onto General Electric as CEO. He is brilliant.

Exploit the Instinct to Complain

Everyone has pent up frustrations, whether they are with their coworkers, bosses or significant others. They will unlikely go directly to their boss and tell him what an idiot he is. However, they will welcome a release. If probed, they are likely to share their frustrations with someone they believe they can trust not to disclose their comments.

Elicitor: What are some of the frustrating challenges you have when working with your senior management?

Target: I generally get along with everyone, except with my direct supervisor. She seems to take direct personal credit for any success by our unit and shifts blame to her subordinates for any failures. I'm sort of tired of making her look good.

Word Repetition

By repeating back the same word or phrase that the target has used, the elicitor will usually create a need for the target to provide further elaboration.

Target: Last year our sales were down by 54 percent.

Elicitor: Down 54 percent?

Target: Yes, this is very unusual after six straight years of strong growth and is largely attributable to the rollout of a similar product by Chinese firm Huawei.

Quotation of Reported Facts

Here the elicitor is drawing upon something that was already reported in the press.

Elicitor: I read in the Wall Street Journal that several of the largest U.S. banks were having difficulty in complying with the new U.S. Treasury reporting requirements identifying offshore accounts held on behalf of their customers.

Target: Yes. As you can imagine, confidentiality for our clients is a delicate matter. If we cannot ensure confidentiality, some of the clients will look to other financial institutions, which tend to circumvent these requirements.

Naiveté

When the elicitor expresses a lack of understanding about something they have experienced or learned about, it encourages the target to be helpful as a mentor to the elicitor on the subject.

Elicitor: I just don't understand how trade policy decisions like raising tariffs on imported Chinese goods will help your company increase its sales in the domestic market.

Target: Currently, our closest competitors are from China due to their very low labor costs. A 25 percent increase in tariffs would force these competitors to either lower their profit margins or increase their local prices.

Criticism

Here the elicitor will criticize something that the target has an opinion on. It will allow for the target to share the same criticism or to provide their own view, which might serve as insight.

Elicitor: The company's extensive research and development activities into self-driven vehicles is an absolute waste of resources. This will never be successful.

Target: Actually, they have conducted a lot of surveys on this topic. The survey results tend to indicate that most people, especially those between the ages of 18 and 35, acknowledge that they would be open to using this technology as long as certain safety standards are met.

Feigned or Real Disbelief

While somewhat similar to the quotation of reported facts, here the elicitor will express dismay or disbelief that the reported information is true in an attempt to get the target to explain that it is true and why.

Elicitor: There is no way that the firm's latest acquisition of Alliance Technologies will be profitable.

Target: Actually, it does not appear profitable if we only look at the balance sheets. However, the real goal is to eliminate one of the biggest competitors in our market. We will then be able to improve upon our profit margins by increasing our prices while lowering many of our production, distribution and marketing costs.

Purposefully Erroneous Statement

The elicitor will make up a false statement and attribute it to something they may have heard or read, and the target will usually take the opportunity to set the record straight.

Elicitor: I heard a news commentator state yesterday that United Airlines was having severe financial difficulty and was in the process of filing for Chapter 7 bankruptcy.

Target: You must have heard something wrong. This is impossible. United is very healthy financially. In fact, they just placed an order last week for an additional 35 aircraft from Boeing.

Mirroring Personal Discussion

This approach is exceptionally useful when trying to obtain basic information from someone who the elicitor has just met.

Elicitor: I can't wait to get back home. I have already missed my son's last two soccer games and my daughter's piano recital. And you, do you have kids?

Target: Oh yes, I have two boys and one girl.

Elicitor: Kids are great. How old are they?

"My Friend John"

Here the elicitor will make up a story that they heard and attribute it to a friend or family member who ostensibly made the comment.

Elicitor: My brother-in-law, John, works as a researcher for Magnum Defense Industries. He says that his company recently adopted many intrusive policies affecting their employees. They must receive prior authorization before travelling overseas and report all their foreign contacts. They are also subject to random searches of their briefcases and handbags. Is this normal in your industry?

Target: It varies from company to company. We don't require employees to obtain approval prior to travel. However, they must file a report after returning from such a trip. It includes reporting any foreign contacts made with whom they plan to have a sustained relationship.

◆◆◆

There are additional considerations for social engineers regarding elicitation and the use of these techniques. First, while very effective, no technique should be overused. It is best for the elicitor to make use of mix of techniques during a conversation in order to avoid any suspicion from the target.

Prior to each planned encounter with a target, I would map out the goals of my conversation. This would usually include five or six specific points I wanted to gather information on regarding the individual or their organization. For each of the points, I looked at what specific elicitation technique I could use to introduce the topic. I then considered how I could manage a logical flow of the overall conversation to cover all points. It never ceased to amaze me on how easy it was to elicit very sensitive information from people who barely knew me.

Enhanced opportunities for elicitation can be leveraged when conversing with the target in a variety of venues to include their office or residence as well as other locations far removed from either. In the case of the office and residence, targets will have artifacts on display, which present insight into what is important to them while offering a convenient pretext on which to ask a question. At the office, the target will likely have pictures of their children as well as framed accomplishments such as university degrees, professional certifications and other recognitions. The elicitor may also experience how this individual interacts with their boss or staff.

At the residence, the elicitor may experience the target's interactions with their spouse and children. He will be able to assess the social status of the target as well as identify hobbies and other interests.

At a third location removed from both home and office—especially in more social settings—the target may be much more relaxed and talk about their feelings relating to their professional and

family situation. And of course, the more alcohol consumed, the more talkative the targets can become.

A key determinant regarding whether a target will share sensitive information during an elicitation is whether or not they consider the information to be truly protected. The signing of nondisclosure agreements and clear marking of information as restricted confidential information will likely resonate and impede targets from disclosing it. However, if the organization does not have in place a system to classify information, the employee might

not appreciate the true value of the information for an adversary.

Chapter 7

Channels for Manipulation: The Art of Phishing and Smishing

"If you believe everything you read, better not read."

—Japanese Proverb

The extensive work that is conducted to select a target entity, collect open-source intelligence on that entity, identify potential insiders and establish contact with them is only one portion of a social engineer's scheme. Now that they have built an assessment profile or even gained the trust of the target, it's time to use various communication channels to effectively manipulate them.

These channels are best categorized into the following four approaches: email (phishing), SMS text messages (smishing), voice call (vishing) and good old-fashioned face-to-face encounters. Phishing and smishing, the most common digital manipulation tools, require a similar carefully crafted yet passive approach. Vishing and face-to-face encounters will be discussed in Chapter 8.

Phishing

According to cybersecurity experts, email phishing is currently the most prevalent channel used by social engineers to breach security. An attacker sends an email to his intended victims containing a link or attachment that the recipient is encouraged to open. Clicking on the link may lead to downloading malicious code or prompting the recipient to disclose login information such as usernames, passwords, pin codes, account numbers or other sensitive data. Likewise, the opening of the attachment may release malware into the computer. The typical phisher will design an email that can be sent to thousands of potential victims. The email will appear to come from an institution that most members of the public may already have a relationship with.

One common approach to phishing involves an email alert from a financial institution such as Bank of America. Since a large percentage of the population has an account with Bank of America, most recipients will take note of an email that appears to be coming from that bank. Typically, such an email will advise of an alert regarding suspicious activity on the recipient's account, claiming that the

account is frozen until the transaction can be verified. The email will contain a link for the recipient to click to directly log into their account. Once the recipient fills in the fields of username, password and additional security information such as account number, date of birth or social security number, the phisher has all the information they need to immediately take over the victim's account.

Basing a phishing email on ecommerce is another common tactic. Almost everyone has made purchases on Amazon at some point, so the phisher sends out a blanket email with confirmation of the processing and shipment of an order. The email contains a PDF attachment with the full details. If and when the recipient clicks on the link to open the attachment, malicious code is introduced into the computer.

Another common tactic is masquerading as a popular online service such as Netflix. The phisher sends out an email appearing to come from Netflix stating that payment was declined from the credit card on file for the account. The email contains a link to update payment information and requires entry of the user's full name, credit card number, expiration date and security code. Once again, the phisher has all they need to compromise the credit card.

In addition to these traditional examples, social engineers will also take advantage of recent events that are captivating the general public. At the time of this writing, the world was experiencing fear and panic regarding the spread of COVID-19. There were many cases of phishing emails sent out by criminal organizations leveraging the crisis, targeting anxious and unsuspecting recipients and claiming to provide updated information. Each of these emails provided a few introductory paragraphs along with a link for additional information. Unfortunately, many individuals fell victim by clicking on such links.

Spear Phishing

I occasionally encounter people who will comment that they are not so naïve as to fall for these mass-marketed gimmicks. While congratulating them on their basic email hygiene, I then caution them that phishing emails are not always so basic. In fact, professional social engineers looking to breach a high-value target will often deploy spear phishing methodology.

Compared to basic phishing, which is like casting nets from all sides of the boat and playing the odds that several fish will likely be caught, the carefully crafted "spear" is flung with exceptional precision, almost guaranteeing that the intended target will fall victim. Why is it so precise? The email was crafted from the target's personality assessment profile, which was formulated from online social media data. The investment in time taken to research the target and design this approach is minuscule when criminals are looking at netting thousands, if not millions, of dollars from the breach. Spear

phishing attacks have become increasingly common in a variety of industries.

To illustrate this approach, say some criminals have decided to breach Diamond Utility Corporation (DUC) to obtain data on their customers. After careful study, they have decided to target Randy Wilton, who is DUC's senior data analyst. When gathering data for his personality assessment profile, they learn that Randy has a passion for collecting rare stamps, coins and documents. Based on this assessment, they send him an email announcing the upcoming auction of an authentic copy of the Declaration of Independence. While 200 were printed on July 4, 1776, only 26 copies survive today. Randy's knee-jerk reaction will be to click on this link, not thinking that it might be a phishing attempt. Once he clicks on the link, the criminal group compromises his computer and eventually his company's entire network. After stealing customer data, the criminals pursue a bonus by installing ransomware, effectively shutting down the power supply to these customers until DUC pays the requested $3.1 million ransom.

Another example would be if a foreign intelligence service was looking for a way to breach the security of the U.S. Department of Defense (DOD). They would assess that targeting a new state-of-the-art DOD facility being built over the next 18 months might give them an opportunity. While directly penetrating this facility would be next to impossible, they decide to look at several of the outsourced firms contracted for the buildout. They identify Kline Engineering Consultancy Services (KECS) as a potential target. Within KECS, they identify CEO William Kline as their priority inside target, and considerable information on the CEO is gathered from social media accounts and other online sources. His personality profile assessment reveals that one of his top passions is sailing—he often posts pictures and comments highlighting outings with family and friends on his 250-foot sailboat. On more than one occasion, he has commented that one of his dreams is to someday sail the Mediterranean.

The intelligence service decides to craft an email appearing to come from his local sailing club. The email announces an upcoming sailing excursion to the Mediterranean with limited availability, and attachments are said to contain additional information such as pricing and registration forms. Although he has received basic phishing awareness training, William immediately downloads the attachments for more information. In addition to believing that he can trust an email appearing to come from his local sailing club, he does not want to miss out on an opportunity to pursue his lifelong dream. As a result, William's laptop is immediately compromised with malware. In addition to storing sensitive information on this laptop, William also uses it to access his firm's server. The foreign intelligence service is

now one step closer to achieving its objective of breaching the DOD's new facility.

Another variation of a spear phishing email would be the social engineer's creation of a fictitious LinkedIn account to engage a target, Robert Franklin, a senior project manager for the Allied Health Network (AHN). From his LinkedIn profile, the criminals learned that Robert is a member of the Freemasons. Given the fraternal nature of Freemasons, they assess that Robert will likely accept an invitation to connect coming from someone who claims to be a fellow member. Once they have connected and exchanged a couple of messages, the social engineer sends an email to Robert with an attachment and asks him to open and review the attachment. Robert trustingly opens the attachment, releasing malware and infecting AHN with ransomware. As AHN cannot afford any delay in accessing patient records and wants to avoid any blowback to their public reputation, AHN agrees to pay $6.5 million in bitcoin to secure the decryption code.

I occasionally come across someone who tells me, "Nah, most people will not accept invitations on LinkedIn from people they do not know." Based upon my own personal experience with LinkedIn, I would strongly argue that most people do accept such invitations. Frequently, they will not even bother to review the LinkedIn profile of the requester—they are only interested in expanding the numbers in their network. Furthermore, if a professional social engineer is concerned that the target might not accept such a request, they can first invite people from the target's network to connect before extending the invitation. Such connections include coworkers, industry peers or members of the same professional organization. Once the target sees that several people from their own network are already connected to this fictitious account holder, they will likely accept.

LinkedIn is not the only social media platform that can be used to deliver a spear phishing attack. Practically any platform that allows users to send and receive private messages can be leveraged to deliver malicious links or attachments. That includes Facebook, Instagram, WhatsApp, Twitter and WeChat, just to name a few. Due to the general public's increasing use and trust in social media networks, along with the ease in creating fake profiles for anonymity, such platforms will likely replace email as the channel of choice for professional social engineers.

Smishing

Back in early 2002 when I was living in France, I was amazed by the popularity of text messaging throughout Western Europe. While it was not so common in the U.S. at that time, it was only a few more years until it eventually became one of the principal means of

communication in America. In some cases, it is even a more effective way of communicating than traditional email. People receive dozens, if not hundreds of emails on any given day. Unable to read them all, they will typically read the title lines before deciding to read, ignore or delete. Text messages, however, seem to get much more attention. In addition to receiving fewer of them, many people will have alerts activated for incoming text messages. As a result, they are likely to take a closer look at the contents of each text message received. Marketing companies have recently incorporated the use of text messages, fully realizing that they have a much higher click-through rate than standard emails. Social engineers, also realizing this trend, have now incorporated smishing into their toolkit.

In the context of social engineering, smishing is actually very similar to phishing. However, instead of using an email, the social engineer will send a link or document file via a text message. The result is the same. Once the link is clicked, or document file opened, the attacker has breached the security of that mobile device. Smishing is named for the SMS messages used to carry out the scheme.

Say a criminal group was able to purchase on the dark web a digital employee telephone directory for Maximus Worldwide Travel Services (MWTS). They develop and send to several employees over a three-day holiday weekend a text message appearing to come from MWTS's HR department. It advises that there is a potential technical problem regarding the upcoming payroll, and recipients are instructed to immediately open the attachment, which will provide information on what they need to do to avoid a disruption in their pay. Playing upon emotion and the sense of urgency in avoiding a delay in pay, most of the recipients will immediately open the attachment. Upon doing so, they will compromise their company-issued mobile devices, which are also used to access MWTS servers. Because the attack happened over a holiday weekend, it will take several hours before MWTS management will realize that there may be a compromise.

Smishing is especially effective against people who use their mobile devices to conduct the bulk of their day-to-day communications. Rebecca Miller is the owner of one of the largest real estate agencies in South Florida, and she is constantly dealing with established clients and frequently receives referrals from them. After conducting minimal research, the social engineer easily obtains her mobile telephone number and the names of several former clients. He then crafts a text message falsely claiming that he was referred to Rebecca by one of her clients. The text message includes a word document identifying a listing of interest. Rebecca downloads this document and never realizes that it contained malware, which allows the social engineer to eventually gain access to her firm's database.

The prize is information on the financial transactions of clients for the previous 10 years.

Phishing and smishing are passive communication tools sent by social engineers to their intended victims for the purpose of enticing them to undertake the simple action of clicking on a link or opening an attachment that will download malware. In addition to compromising the victim's computer or mobile device, these tools can potentially compromise an entire network.

Chapter 8

Channels for Manipulation: The Art of Vishing and Face-to-Face Encounters

"We only see what we want to see; we only hear what we want to hear. Our belief system is just like a mirror that only shows us what we believe."

—Don Miguel Ruiz

Vishing

Compared to phishing and smishing activity, which is considered passive communication, vishing is an active and dynamic social engineering technique that uses the telephone to directly engage with the target. While vishing will seldom directly result in a security breach, it can play an important, and sometimes crucial, role in executing more elaborate security breach attempts. The purpose of the call may be to get the victim to divulge sensitive information such as internal processes or procedures, or it may be conducted to persuade the victim to undertake a specific action, such as modification of their account settings or creation of access passes.

Think of vishing as making a pretext call. To accomplish the objective, social engineers must successfully convince recipients that we are whoever we pretend to be. To increase credibility, social engineers will often spoof the call—using simple technology to manipulate the caller ID seen by the recipient. Using spoofing, I could assume a number of roles when calling a target, such as a fellow employee located at another facility, someone from tech support, the target's investment adviser or someone from the school where target's children attend.

Vishing can take many forms. Say a criminal group is attempting to steal customer data from Quantum Entertainment (QE), a leading provider of online media content. While evaluating several potential insiders, they notice an update to the LinkedIn profile of Christine Belasco, who recently started as a receptionist at QE. Assessing that Christine is not yet familiar with QE policies and procedures and likely isolated from coworkers, they decide to use a vishing approach. The social engineer pretends to be Tom from the IT support team and spoofs the caller ID so that it appears to be legitimately coming from that department. Tom welcomes Christine to the company and

encourages her to reach out to IT for any questions or assistance as needed. He then advises that an anomaly has been detected within her user profile, which will eventually result in a crash. Tom offers to assist Christine by rebuilding the user profile at her convenience. Christine, fearing how a crash could negatively impact her performance at this new job, immediately takes Tom up on the offer. Tom sends her an email with a link to authorize login access to her account. While keeping Christine distracted on the phone, Tom uses this access to create a backdoor into the network, which will be exploited later by his team. Upon conclusion of the 15-minute call, Christine expresses her appreciation to Tom for helping to prevent what could have been a serious disaster for her, not realizing that she had just facilitated a breach that will result in devastating consequences for QE.

Vishing attempts can get exceedingly complex if the social engineer has access to information about multiple targets within an organization. Consider a criminal group that is interested in breaching the security of the Global Health Foundation (GHF) for information on more than 140,000 wealthy donors who contribute a significant portion of its $230 million annual budget. Based upon open-source research, the social engineer has learned that GHF CEO Alex Burton is currently away on travel to Dubai to attend the 14th World Congress on Healthcare in Developing Countries. A complete conference schedule was available online. Research also revealed that when travelling abroad, senior GHF officials always contract a security transport company by the name of Liberty Limo. The social engineer decides to design and execute a pretext call claiming to be from Liberty Limo and requests to speak with Alex's executive secretary, Kimberly Davis. The objective is to get Kimberly to transmit very sensitive data, believing that she is complying with a request from her boss.

Due to the eight-hour time difference between Dubai and GHF headquarters in New York, the social engineer places a call to Kimberly at 0830 (EST). He spoofs the call to show "Liberty Limo" on the caller ID.

Ms. Kimberly? (spoken with a slight middle eastern accent)

Yes?

This is Rashid from Liberty Limo. We are handling Mr. Alex's transport and other needs while he is here in Dubai. Don't worry—he is very fine. He just went into an important meeting and asked me to contact you. He urgently needs a copy of the latest report detailing the names of GHF's top financial benefactors, with their names, amounts donated and their contact information. Mr. Alex requested that it be sent to my email address so that I can immediately print it out and pass to him during his

meeting. He is having some problems receiving incoming emails to his phone.

What is the email address he wants it sent to?

Rashid.LibertyLimo@gmail.com

To further alleviate any concern or suspicion that Kimberly may have, the social engineer further adds:

Ms. Kimberly, Mr. Alex also wants to know what your favorite color is.

My favorite color? What in heaven's name for?

Well, I think he found something from the UAE that he wants to bring back. I can't tell you what it is. I only need your favorite color.

He shouldn't bother bringing anything back for me. My favorite color is purple.

Excellent. I will make sure he knows that. Thanks for the email—I just got it and will immediately pass the report to him.

Vishing with Chat Groups

While not typically recognized as a vishing tool, online chat groups can also be used for the same purpose. One of my university students was finding it very difficult to collect open-source information on her target company. However, she then discovered an online chat group where people freely exchanged information regarding their experiences working for the firm. Using an alias, my student entered the chat posing as someone who was very interested in applying for a position that she had seen on the company's website. Once she connected with a person who just happened to be a current employee from the firm's HR department, she requested that they move their chat over to a private room. She artfully used a number of the elicitation techniques previously discussed to collect considerable information, including sensitive insight into an exploitable vulnerability.

Face-to-Face Encounters

Out of all social engineering techniques, in-person engagement was the approach I most favored during my career as an intelligence officer. It allowed me to fully leverage nonverbal communication, which is nonexistent in either phishing or smishing and rather limited during vishing. For me, effective nonverbal communication included warm handshakes, smiles, direct eye contact and lots of arm gestures.

Likewise, it allowed me to see invaluable nonverbal cues the target displayed, which would help me measure progress in rapport building and gauge their comfort level with me. More importantly, it would help to better determine their comfort level regarding the information I was eliciting, or the action I requested they take on my behalf. It helped me visualize whether I had a green, yellow or red

light. If green, I could push forward and strike while the iron was hot. If yellow, I knew that I would have to take a step back and attempt to better frame the discussion to put them at greater ease. If red, I would have to back away, change the subject and consider other options.

The respective objectives for a social engineer's use of face-to-face encounters can be numerous, but this approach is used most effectively in a few common scenarios.

Facility Intrusions

To gain unescorted access into a target facility, the social engineer will need to develop and artfully execute a suitable pretext to get past gatekeepers such as receptionists, guards and electronic barriers. A common technique is piggybacking or tailgating—tagging along with another person or group of people who are authorized to enter the restricted area.

More calculated pretexts rely upon previously collected information identifying contracted third-party service providers, as well as those establishments making deliveries to the facility. The following are some frequently used roles social engineers might pose as to gain access:

- A member of the contracted food catering service
- A member of the contracted guard force
- A member of the contracted janitorial staff
- Someone working for IT conducting an installation or repair
- Someone delivering flowers
- Someone making a food delivery (local establishment or food delivery service)
- Someone making a FedEx or UPS delivery

In all cases, the social engineer must look and act the part, and props are critical. If impersonating a third-party vendor like those listed above, they must wear clothing that matches the profile. Uniforms are relatively easy to procure on the market or have manufactured. If required, the social engineer will carry a badge or visitor pass easily fabricated based off exemplars seen in photographs uploaded to social media by employees from the workplace. If delivering flowers, they will carry a nice flower arrangement as well as the name and location of the person the flowers must be personally delivered to. They will know what occasion the target is celebrating, such as a birthday or anniversary, based on Facebook posts. If claiming to be from IT, they will carry a small tool kit.

What does the social engineer do once inside? Unescorted access inside a facility offers several options for technical exploitation:

- Placement of audio devices in conference rooms to pick up confidential discussions during meetings.
- Placement of keyloggers on computers to collect usernames

and passwords.

- Distribution of lethal USBs, such as malware-infected USBs labeled “Confidential Payroll.” The social engineer will leave each one in an area where an employee could pick it up. While some of the employees might turn the discovered USB over to the HR department, it is almost certain that at least one of them will first insert it into their computer system out of curiosity. Once inserted and the corrupted file opened, the compromise is initiated.

I once had a requirement to gain access to a target office for the purpose of obtaining a floor plan. This plan would be used by a team that would later conduct a surreptitious entry in the middle of the night to place electronic eavesdropping equipment. The targeted office occupied the entire eighth floor of a 10-story office building.

Using the pretext that I was interested in available office space, I contacted the building’s management office by telephone. They provided me with an appointment to visit available office spaces located on the third and ninth floors. This appointment allowed me to pass security controls and access the building. Upon reaching the management office, I met with Rebecca. We discussed the general services provided by building management, and I requested and obtained a copy of the generic floor plan structure common to each floor. Rebecca then led me on a tour of the building, including the two available offices. As we finished on the ninth floor, I politely wrapped up my visit. I told Rebecca that I would give her a decision within the next few days. I excused myself to go to the restroom on that floor prior to seeing myself out of the building.

Upon exiting the restroom, I took the stairwell down to the eighth floor and entered the reception area of my target office. I explained to Jason, the receptionist, that I would likely be a new tenant taking space on the ninth floor. I added that during my tour, Rebecca was highly complementary of the design of the office spaces on the eighth floor and mentioned that they were the best layout in the entire building. As Jason proudly smiled, I asked whether he could give me a quick tour of their offices, and he readily obliged. I made frequent references to the beautiful décor and was granted permission by Jason to take a few pictures. He even introduced me to a couple of his colleagues as someone who would soon be a new tenant.

The information I was able to collect during my visit with Rebecca followed by the tour of the target office was enough to meet my objective. Based upon my pictures and additional observations, I was able to return to the generic map provided by Rebecca and insert the additional details.

Accessing Insider Targets

While it may be difficult to establish a viable means to contact and meet insider targets within their workplace, it is quite easy to target them when they attend outside events, where they are easily approachable and tend to have their guard down.

Professional Conferences

The social engineer will frequently use professional conferences as an effective way to approach identified insider targets as well as targets of opportunity. In advance of the event, the social engineer may be able to obtain a list of entities that will have representatives at the event. Upon arrival, the social engineer will aggressively work the floor, looking for name tags of potential targets and orchestrating brief encounters during lunch or coffee breaks. Once engaged in a conversation, the social engineer can establish rapport with a potential target and use elicitation techniques to collect information on the insider and their employer.

Conference Speakers

Insiders may be invited as guest speakers during a conference event, creating a unique opportunity for the social engineer. The speaker's biography will be made available, as well as the presentation topic and date and time of the presentation. In this case, the social engineer will predesign a specific pretext for contact with the speaker, which will typically take place at the end of the presentation. While this initial contact is very brief, it will set the stage for a follow-up meeting. Even if the social engineer does not physically attend the event, they can use the pretext of having been present and contact the target later to request an opportunity to meet.

A variation to targeting a conference speaker is targeting someone who is teaching a multi-session course, either at a university or on behalf of a professional association. On a couple of occasions during my CIA career, I was able to identify well-placed insiders from high-priority target organizations who were giving lectures. In both cases, I signed up for the course and arrived at least 20 minutes early on the day of the first session. While the participants usually do not arrive until a few minutes before class, the lecturer typically arrives at least 30 minutes early to set up the venue. I would take advantage of that time to introduce myself and establish initial personal rapport. I could then gradually reinforce this connection during class breaks and remaining course sessions.

Networking Events

A diligent social engineer will identify social clubs or professional associations in which their target is a member. Upcoming events can be used for networking opportunities with the goal of either meeting the target directly or identifying someone who knows the target and can provide a referral.

Social Facilitators

At times, a social engineer will orchestrate an event with the sole purpose of getting the target to attend. They will contract with a third party to ostensibly sponsor a private event and provide the facilitator with an extensive list of individuals to invite—including the target. The social engineer will attend the event and use the opportunity to casually start up a conversation with the insider during the event. As this is a rather elaborate and costly scheme, it would only be used with hard-to-access priority target insiders.

Headhunter or Executive Recruiter Scheme

Some companies will manage the complete HR process for hiring personnel, while others may outsource some of the functions to a third party, often referred to as a headhunter or executive recruiter. A typical headhunter will search for prospects who might fit the profile of the candidate sought by the client. They will use several resources such as resume databases, networks of contacts and LinkedIn. When calling a prospective candidate, they may provide general background regarding the client as well as the position, but typically will not reveal the name of the client until further into the interview and evaluation process.

Posing as an executive recruiter is one of the best covers used by successful social engineers. The social engineer will initiate contact with the target via telephone as a headhunter working to fill a position with an unidentified client, describing a position that is a step up from the target's current job, whether in compensation, title or level of responsibilities. The social engineer will mention that they were attracted to the target based upon her impressive resume or profile on LinkedIn and offer the opportunity to get together for coffee to conduct a basic interview. Even when targets are not actively looking for new employment, they typically jump on this opportunity due to a natural curiosity to learn more about the market and what they might be worth. In their minds, they have nothing to lose.

The social engineer uses this interview to collect considerable information about the target and their employer alike. In some cases, a target may be pursued for sensitive information relating to a former employer. In addition to direct interview questions, the social engineer artfully uses elicitation techniques to desensitize the target regarding the attempt to obtain protected information.

While this could be a one-time encounter, it frequently leads to follow-up meetings over coffee, lunch or dinner. The target might even be offered a confidential consultancy agreement to provide insight into the industry and inside information regarding the activities of the target's employer.

Such consultancy arrangements can continue for many months, if

not years. They usually terminate when the "client" no longer has a need for additional information or when the target loses access due to a change in position or retirement. Typically, the target's organization never becomes aware of this devastating and ongoing breach.

The Consultant Scheme

Compared to the headhunting scheme, this is less complex but can yield a similar outcome. Here, the social engineer will typically contact the target insider by telephone, identifying as someone who works as an industry consultant. The "consultant" needs particular insight for a new project that the target may have based upon an alleged referral or their bio on LinkedIn. This scheme will typically only work on those individuals who are motivated by mentoring and teaching. As a lure for ongoing discussions, the social engineer may entice the target with lavish dinners, entertainment, gifts and even financial compensation.

The Desperate University Student Scheme

This is an easy way for a social engineer to directly interview an insider for information under the pretext of needing to complete a research paper or thesis. While conducting the interview, the social engineer will creatively incorporate elicitation techniques to procure sensitive information. It is typically a one-time encounter and can be conducted in person or over the telephone. Insiders are often receptive to this ploy because they remember what it was like to be a university student and want to help. This is especially the case when the social engineer claims to be studying at the insider's alma mater.

The Honey Pot or Romance Scheme

While occasionally encountered in the U.S., this scheme is often used overseas by both intelligence services and criminal groups. Foreign businessmen who arrive in the country to conduct meetings or conferences are prime targets. An attractive female, working under the direction of the master social engineer, will circulate in the vicinity of the target—often in their hotels or nearby restaurants and bars—and attempt to lure him into a conversation. The ignited chemistry will typically evolve into sexual intimacy.

In addition to eliciting information from pillow talk that is passed on to the social engineer, this scheme can leave the insider very vulnerable to extortion attempts. In exchange for regaining control over compromising material such as photos or videos, the target will have to provide specific and damaging information about their organization. Another variant to this scheme would be the social engineer threatening physical harm to the "love interest" or her family unless the insider agrees to the demands. In either case, this scheme is quite effective.

Chapter 9

How Organizations Can Mitigate the Risk of a Security Breach

"Where my reason, imagination, or interest were not engaged, I would not or could not learn."

—Sir Winston Churchill

The types of threat actors that use social engineering, how they choose their targets, what they are after, how they prepare for an attack and the different methods they use to manipulate insiders to achieve their goals all take a variety of forms—each of which can inflict irreparable damage on an organization. While there are so many variables to the threat of social engineers, there are steps organizations can take to significantly decrease the risk of falling victim to such schemes.

Awareness and Realization

Developing an awareness within an organization that social engineering threats do exist is a starting point to defending against them. However, just as important as awareness is a genuine realization that no one person or organization is immune from becoming the target of a breach attempt. Despite the daily bombardment of news stories regarding massive database breaches, ransomware attacks and identity thefts, many organizations and individuals believe that it will never happen to them.

This mindset is extremely dangerous and makes individuals as well as organizations very vulnerable. Essentially, they become soft targets. For criminals, there is no reason to pursue harder or more secure targets when soft ones abound. Ironically, most soft targets only actively pursue hardening their security posture after suffering firsthand from an attack, much like a homeowner waiting for their house to become burglarized before installing an alarm system. This type of response is reactive instead of proactive.

As the human factor is shown to be the weakest link in overall security and data protection, this is where the greatest focus on prevention needs to start, from contract employees all the way up to the C-suite. Spending millions of dollars in technology to harden the physical facility or IT network is meaningless if human actions,

whether intentional or innocent, circumvent protective controls. This is where security awareness training is crucial.

While most organizations have developed security training programs for regulatory compliance reasons, it frequently ends up being a mere exercise to check the box. As a result, many organizations look for inexpensive off-the-shelf, on-demand training programs to meet compliance requirements. Employees take this annual mandatory training at their desks, clicking through the program while multitasking and generally find little personal value in the program. As a result, the process increases a false sense of security for the organization and reinforces the employee mindset that security awareness training has little relevance for them.

True and effective security awareness programs need to start with the individual employee—it is crucial that they understand and appreciate how appropriate security measures can personally protect them and their loved ones from both physical and financial harm. Once they buy into the value of security at a personal level, they will more readily bring the same awareness mindset to their role within the company.

Effective awareness training must extend well beyond conditioning employees on whether to click on a link in an email or following a checklist of dos and don'ts. All staff employees and contractors need to fully understand the bigger picture, taking pride and ownership of their valuable roles in protecting the organization, its customers and fellow employees.

Hands-On Training

After my days of gathering intelligence for the CIA ended, I couldn't stop thinking about the ways social engineering techniques are used by threat actors of all types on ordinary people and organizations. I decided to put my years of experience to use by training people and organizations to avoid becoming unwitting insiders like the countless people I targeted in my career.

I enjoy conducting interactive educational workshops onsite through the Counterintelligence Institute and engaging employees on the information their organization holds that might be of value.

- What technology, customer information or employee data might threat actors seek?
- Who might want to steal it and for what purpose?
- Where is that information held within the organization and who has access to it?
- In addition to financial losses from a breach, what impact might it have on the brand's reputation?
- Might the organization be vulnerable to a ransomware attack?

- If so, what would the impact on their operations be?
- In such an event, should they pay the ransom or refuse?
- Can they imagine scenarios in their company for a business email compromise?
- Might their organization be an attractive target to gain access to a customer organization that might be even more alluring?

I then lead them through a hands-on exercise where they search for open-source information regarding their organization and discuss the value of such information to someone planning a breach. This includes the identification of potential insiders—what departments or employee roles within the organization could serve as attractive targets? I next focus on the use of social media for collection on insiders, and I have each employee conduct a self-assessment of their own social media profile.

The workshop continues with examples of various social engineering techniques and a discussion regarding ease or difficulty of their successful use within their company. Based upon my experience, this approach to training transforms the way employees think about security and results in greater awareness, both at the organization as well as in their own personal lives.

One of the most important ways an organization can mitigate the risk of a security breach is by minimizing the amount of information made publicly available regarding the entity and its employees. All posted information, whether on the organization's website or social media sites, should be evaluated prior to its dissemination to the World Wide Web. Is its public relations value greater than its potential use by someone trying to breach the organization's security? Many times, the answer will be yes. However, there are also many occasions when the information posted provides little added value to the organization's public reputation yet presents serious vulnerabilities to its security posture.

In addition to sensitizing employees regarding what information should not be posted online, the organization should have someone whose function is to regularly conduct extensive searches on the internet, including the dark web, to identify anything that could pose a security concern. Once identified, management will have to ascertain whether the information can be removed. If it cannot be removed or might remain in an archived version of the internet, the potential use of this information by nefarious characters needs to be evaluated, along with suggested safeguards.

In addition to concerns about controlling the amount of information available that may be exploitable by social engineers, organizations and their employees must always be ready to confront

attempts to breach security by recognizing the warning signs.

Warning Signs: Phishing and Smishing Attempts

Phishing via email and smishing over SMS messages are the two communication mechanisms that will often contain links or attached files. Here are several things to consider:

- Don't trust the display name or heading when receiving an email. It is more important to focus on the actual email address from which it is coming—anyone can copy and paste logos.
- Realize that email addresses, just like telephone caller IDs, can be spoofed.
- Are you the only recipient, or is there a list of recipients?
- Is the email addressed specifically to your name, or is it generically addressed "Dear Valued Client?"
- What is the actual content of the message? Is it requesting that you take urgent action because of a problem? That is a big red flag. Is it asking for personal information? Another huge red flag! Does the content make sense? Does it contain grammatical or spelling errors? If so, it is likely fraudulent.
- Review the signature—the lack of details about the signer is an indicator of phishing. Companies will not only have a name, but also an address, contact phone number, email, web address and more.
- Before clicking on any link, scan URLs to see whether they match the name of the source. By hovering your mouse over the link, the URL will show on the bottom of the browser or in a pop-up box. To test the link, open a new browser window and type in the website address directly rather than clicking on the link.
- You must never click on a link or open an attached file provided in any email that you cannot completely trust, especially those asking for you to log into your account from that email. You can always open a separate browser to directly log into your account and ascertain whether the information provided is correct. Remember the example of Randy Wilton in Chapter 7 who received an email regarding the upcoming auction of a rare document? If true, Randy would likely be able to find available information on the auction by conducting a simple Google search.

Warning Signs: Vishing or Face-to-Face Attempts

The following are potential warning signs of a breach attempt during phone calls or face-to-face interactions:

- Refusal by the caller to give a callback number
- Making an out-of-ordinary request—something not standard or normal

- ➢ A claim of authority from a boss, someone representing the boss, security or law enforcement
- ➢ A message that stresses urgency and requests that action must be taken immediately
- ➢ Someone who threatens negative consequences of noncompliance such as jeopardizing your job
- ➢ Someone who shows discomfort when questioned, such as hesitating to respond or stuttering
- ➢ Someone that name drops and appears to know everyone, including use of referrals
- ➢ The excessive use of compliments or flattery
- ➢ Someone who is inquisitive about you or your employer
- ➢ Asking questions that are out of context of the purpose for the meeting or casual encounter
- ➢ The information provided by the person regarding the nature of their job or business does not appear fully credible

In all cases of suspected social engineering, it is extremely important to verify the identity of the requester as well as the legitimacy of the request before complying with the action. Remember, they are approaching you with the request, whether by email, text, telephone or in person. If they have targeted you, they have done their homework and can be extremely convincing.

To verify the authenticity of an interaction, consider the following steps.

In the case of email or SMS: Do not automatically click on the link or open the attachment. If the message was received from an organization, go directly to their website. In the case of receiving the communication from an individual, telephone that person.

In the case of a telephone call: Do not comply with the information requested. Instruct the caller to make the request in writing. Alternatively, ask for a callback number and return the call after allowing some time to pass.

In the case of someone trying to enter the facility: Follow your company's strict policies regarding access to your facility. If they do not have a proper access badge, direct them to the issuing party. If their badge requires an escort, do not allow them to proceed without one. If their badge only allows access to certain areas within the facility, do not allow them to enter restricted spaces. Make no exceptions. For those issuing the badges, make sure there is a written request by an authorized official and that it was received via a secure channel. Never issue one based on a phone call, which can be susceptible to vishing.

In the case of being approached by someone during conferences, trade shows or other locations where you could be targeted: Never

discuss proprietary information with them. Be alert to potential use of elicitation techniques. Take control of the conversation and use counter-elicitation to ascertain their credibility. Try to obtain any information from them that may contain verifiable information (brochure, business card or references).

If contacted by a headhunter: Before agreeing to personally meet, request specific information that may be verifiable to include full name, company name and office telephone number. Google the company's name to see whether there is any mention of this company beyond their own website.

Incident Reporting and Reinforcing Security Awareness

Employees should understand that simply not complying with a request coming from a suspected social engineer is not enough. It is extremely important that they report the incident to their organization's security department, which will be able to track any patterns or trends from incident reports and help validate whether the organization is the target of a true attack. When employees fail to report such incidents, they are giving the attacker another opportunity through someone else.

Employees need to understand that they are truly the first and best line of defense for safeguarding the organization. Failure to do so could result in the loss of trade secrets, customer data, employee data, revenue and potential loss in employment.

Consider adapting a slogan that is easy to reinforce and remember, such as "verify before trust." This approach should be encouraged, and employees should never be admonished for taking added measures in protecting the integrity of the organization's security.

To maximize the effectiveness of a security awareness campaign, it is important that training be reinforced by ongoing practical exercises. Whether conducted inhouse or through the support of a third-party vendor, employees need to be randomly tested in all four of the communication channels used by social engineers, and results and trends need to be analyzed by management. Individuals who properly shut down the attempted social engineering ploy need to be recognized and rewarded. Those who fail should neither be chastised or publicly named. However, it is important to share the results of these tests with the entire workforce on a regular basis.

Chapter 10

Taking it Home: Safeguarding Your Personal Information and Financial Security

"No one has power over you unless you give it to them, you are in control of your life and your choices decide your own fate."

—Anonymous

Individuals need to be cognizant that they can easily be targeted by a social engineer for direct personal exploitation or as potential insiders for gaining access to their targeted organizations. Just as organizations need to exercise care when disseminating information to the public, individuals have to exercise that same caution and discipline in not releasing exploitable information that can make them vulnerable as potential targets.

The news media regularly reports on major security breaches suffered by corporations, nonprofit organizations, and academic institutes as well as city, state and federal government offices. In comparison, there are rarely reports regarding individuals who have been directly victimized by ransomware or identify theft. That doesn't mean such cases are rare, however—they are just as frequent as successful breaches at organizations. The difference is that they are not publicly disclosed.

To put this in perspective, consider the decision process for organizations and individuals regarding whether to report a security breach. It boils down to legal requirements—organizations are only required to report a breach if it resulted in the potential disclosure of personally identifiable information. These rules are subject to individual state regulations and will depend upon the location of the breached company, as well as location of individual consumers who have had their information compromised. A second regulation comes from the Security and Exchange Commission (SEC), requiring that all publicly traded companies report the breach if it has a material impact on shareholders.

When not required to do so by regulations, an organization will typically decide not to report. They are concerned that the disclosure of security breaches will negatively impact their reputation and brand. As a result, there are many more cases of data breaches suffered by

organizations than what is reported.

Likewise, individuals are not legally required to report a breach of their personal laptop. They are encouraged, however, to file a report with the Federal Trade Commission (FTC) if they are victims of identity fraud. A copy of that report, as well as one issued by the police, are frequently required when dealing with merchants who may have issued credit under the stolen identity. While the FTC received more than 650,000 reports of identity theft in 2019, these reports are never released to the public.

In addition to identity theft, social engineers will also target individuals with ransomware. While criminals will demand much less money from individuals compared to the ransom of enterprise data, it can still cost the victim several thousand dollars. Another increasingly popular extortion technique is demanding payment in exchange for not publicly releasing compromising photos or sexually explicit emails secured from a hack. While many cases of "sextortion" schemes are ultimately hoaxes or empty threats, victims are terrified and frequently pay to avoid reputational or legal problems.

Assess Available Information

The very first step an individual should take is to assess what information they have already placed on social media and the measures taken to safeguard it. Have they posted details such as their full date of birth, upcoming vacation plans, travel itinerary or identifier information regarding their children? If so, this is extremely exploitable and should be removed. While it is unrealistic to recommend that people not use social media, the risk of potential exploitation will be reduced if proper privacy settings are put into place. Individuals must review the privacy settings for all their social media accounts on a recurring basis. When privacy settings are not restricted, social media users are opening themselves to the world. The less information publicly available about a person, the less likely they will become an actual target. Most public information on an individual is shared by the individual themselves on their published profile and postings on social media, giving social engineers considerable control.

Individuals must also consistently evaluate the provision of information to those who ask for it. The internet presents frequent opportunities for individuals to obtain free products or services in exchange for filling out a registration form requesting personal information. In such cases, it is important to verify that the organization requesting such information is legitimate. One of the oldest techniques for collecting information over the internet is enticing an individual to provide information during a registration process for a chance to win a prize. Unless you can verify the

legitimacy of the organization behind the event, providing such information is very risky.

Maintaining control over your information should be done in all facets of your day-to-day life. If you are filling out background information at the doctor's office or for another service provider and they are asking for your social security number, stop and ask them why they need it—in most cases, they don't. Don't automatically provide sensitive personal data because there is a line for it on the form.

Carefully Screen Messages

In addition to measures taken to safeguard personal information, individuals must be vigilant in how they respond to incoming emails, text messages, telephone calls and even knocks at their front door, as these approaches can be used by social engineers to compromise security.

Today, most of us carry mobile devices to check our email, search the web, engage in social media platforms and make calls. Many of us use the same devices to gain access to our office's network server. As a result, criminals are increasingly targeting personal mobile devices to gain access to an organization's sensitive data. Even if an individual believes they have nothing personally worth stealing, they should think again—they can become a conduit to their employer.

Mobile devices are especially vulnerable when using public or unprotected WiFi hotspots. If you are logging into sensitive accounts such as your office server, bank account or healthcare portal while on these hotspots, you are taking a big risk—your usernames and passwords can easily become compromised. Be especially wary of free internet service provided at places such as airports, restaurants or hotels. Anyone can set up free WiFi and assign it a naming convention that closely resembles the name of the establishment.

Hackers love to obtain the usernames and passwords used by a target to log into their personal accounts. A typical individual likely logs in to more than 25 different online accounts on a weekly basis, making it difficult to have—and remember—a unique username and password for each account login. Most people will create one username and password and use them across multiple platforms, but the hacker only needs to discover one username and password to log in to most accounts. It is important to use unique usernames and passwords for each login platform, and there are a variety of password managing services available to help keep track of them.

When it comes to unsolicited telephone calls, callers can spoof the number from which they are calling and pretend to be whoever they want to be. They will use a variety of persuasive techniques such as authority by claiming to be calling from the IRS or law enforcement.

They may use scarcity and claim that it is a limited time offer. They might even use social consensus, asking you to make a donation to the fallen veterans.

The best tactic for this threat is to not answer any number you are not already familiar with. Let the call go to voicemail and then listen to the voicemail. Most social engineers, including telemarketers, will not leave a voicemail message—they prefer to call back and try to get you on the line, where they can effectively try to manipulate you. If you do happen to speak with someone by telephone who is trying to get you to buy a product or provide information, do not comply. You can always ask for them to send you the information or request via mail. If it is truly legitimate, they should not have a problem in doing so.

Navigate In-Person Interactions

Many of us have received knocks on the door from vendors of products and services including home security systems providers, painters, roofers or landscapers. Did you reach out to them, or are they approaching you? You cannot fully trust who they are or what they are saying. While being cordial, take their information, but make no commitment. If you are interested, take the time to verify their credentials. If they require a state license to offer their services, go to the website of the licensing authority to see whether the license exists and is in good standing. If they provide references on their website or orally, do not trust these references—they can be staged. Look for independent means to obtain a review.

Despite my experience and understanding of social engineering techniques, even I am not always immune to them, especially if they are used by businesses, not malicious threat actors. Several months ago, I was approached by someone inside of a major hardware store who wore a hat with the logo of this store. He explained that they were conducting free home energy audits and wanted to set up an appointment. Trusting the brand name of the store, I decided to schedule the appointment. When called to reconfirm the appointment, I was told that both my wife and I needed to be present. This was an initial red flag for me—it sounded like it might turn into a high-pressure sales attempt.

The representative arrived right on time for the Saturday morning appointment and went over several well-designed charts and graphs to draw us into the mindset that a few minor upgrades could result in considerable savings to our energy consumption and pocketbook. After conducting a 20-minute survey of the home, he wrote up a proposal for three upgrades. While attempting to show how these improvements would pay for themselves within 18 months, I was taken aback by the cost, which was broken down into components and

labor.

While a bit skeptical, I agreed to sign based upon a clause in the contract that gave us three business days to cancel. Following his departure from our home, I immediately got on the internet to research and verify the market price for each of the components. The quote detailed in the contract for the exact same components was 250 percent higher. This infuriated me.

The following Monday, I decided to physically visit the office of this contractor instead of attempting to cancel by phone. As I'm a certified fraud examiner, I decided to wear my jacket with the Association of Certified Fraud Examiners (ACFE) logo on it. Upon arrival, I asked to see the general manager. I was led past a room of approximately 15 employees who appeared to be working the telephones. I told the manager that I wanted to cancel the contract because I was very uncomfortable with its lack of transparency. Without asking me for further detail or trying to convince me to reconsider, he pulled the paperwork and officially canceled the order.

I subsequently lodged a complaint with the hardware store. I was told that they periodically allow contractors to offer services to store customers if the contractor purchases a number of the components through the store. My response was that they needed to better vet such contractors as this incident seriously damaged their store's brand reputation in my eyes.

This incident only reassured me of the need to never fully trust everything said by someone who approaches you. While not working for the store, this contractor leveraged the appearance of a direct affiliation to gain the confidence and trust of unassuming customers. While unethical, it was not illegal—the contract was written in accordance with state law. While I exercised my right to rescind the contract within three business days, the majority of individuals who sign likely don't realize that they paid too much until after speaking with neighbors several weeks or months later. By that time, it is too late.

There have always existed people who try to leverage blind trust and social engineering skills to accomplish their objectives to the detriment of their victims. Today, more than ever, a variety of resources on the internet can be used to help verify, or call into question, their legitimacy.

You are the first and best line of defense in the protection of yourself, your family and your organization. To defeat most social engineering efforts, remember whenever you receive an unsolicited email, text, telephone call or face-to-face approach to verify before trusting.

Chapter 11

The Future of Human Hacking

"Humans should be worried about the threat posed by artificial intelligence."

—Bill Gates

What might we expect in the months and years ahead regarding the continued successful use of social engineering methodology by various threat actors to breach the security of organizations in pursuit of protected data? Unfortunately, unless there is a significant shift in the mindset of security professionals to place greater emphasis on security awareness training for all insider employees and contractors, this will be a persistent and ever-increasing threat.

Of more concern are several evolving factors that will likely lead to an increase in magnitude of such breaches by both criminal groups and state-sponsored intelligence agencies. The first has to do with economic factors. I'm writing this book while in the midst of the COVID-19 pandemic, which will likely lead to a worldwide economic recession. Shortly after economies enter a significant economic downturn, there is always a sharp increase in criminal activity. It hits at all levels, ranging from petty theft, employee fraud and household burglaries to armed robbery and security breaches of organizations to steal valuable data.

As more and more employees and contractors face severe economic hardships, there will be an increasing number of individuals who will be susceptible to becoming malicious insiders. Some of these insiders will have significant training and experience in IT and related technologies. They will also understand the vulnerabilities posed by human interaction with technology and know how this can be leveraged for personal financial gain. While some may decide to take such action on their own, others will be susceptible targets for recruitment by criminal groups.

Even more serious is the potential use of big data by criminal groups and foreign intelligence services for targeting purposes. The first significant data breaches of organizations go back to 2005 and have steadily increased year by year. Imagine the value in being able to harness, triangulate and analyze data—especially personal data—

stolen over the past 15 years. When we consider the more recent OPM and Equifax breaches, this should not be discarded as a farfetched scenario. It is well within the realm of possibilities.

As discussed in Chapter 1, the data stolen from OPM and Equifax has not appeared for resale anywhere on the deep web. That would suggest that it is being held, and potentially analyzed, for future use. The individuals who could be targeted using this information will be extremely vulnerable. Some of them will likely be key U.S. government employees with access to classified information, or in positions to influence decisions of benefit to a foreign power. Others will hold key positions in nongovernmental entities of interest who could be leveraged to conduct additional data breaches or influence decisions.

Finally, it will be very interesting to see the continued evolution of technology and its relationship with humans. While some people fear that advancements in artificial intelligence (AI) will ultimately lead to our loss in control, I believe that we need to look at it in another light. Technology is, and will continue to be, a mere tool used by humans. It is neither moral nor immoral—humans decide how technology will be used. Just as it can benefit the selfish interests of a few to the detriment of society, it can provide considerable benefits to all of mankind.

While technology evolves, basic human psychology remains rather constant. People will continue to have basic needs. They will also continue to experience human emotions as they relate to their environment. Most importantly, from a social engineer's perspective, people will always have motivations and vulnerabilities that can be manipulated.

The perspective danger is how social engineers will harness technology in the manipulation of their targets. Today it is clear—we can directly see how social engineers benefit from using the internet to collect data on organizations and individuals. Communication channels currently used by social engineers such as email, SMS, phone calls (to include call spoofing) and social media platforms are relatively new technological tools that will continue to evolve or be replaced. In the future, AI might reduce or eliminate a social engineer's limitations and vulnerabilities.

Today, social engineers are limited in the amount of targeting data we can collect, and especially the amount of data that we can retain. As a result, social engineers are unable to analyze information they glean during conversations with the target in conjunction with all available information about the topic or individual. We have limited intellectual brain power.

Additionally, social engineers have our own emotions that can

become distractions and sometimes get in the way of our objectives. While we do our best in trying to read the emotions of our targets, we are limited to analyzing their verbal communication in conjunction with some nonverbal cues.

If social engineers are able to harness the use of evolving AI for human manipulation, we can only speculate on the exponential threat. Whether 25, 50 or 100 years from now, man will likely produce robots that will be able to mimic human form. If so, their potential strengths could include the ability to maximize all available data on targets, quickly analyze new data provided by a target and instantaneously be able to formulate and execute techniques to advance manipulation toward overall objectives. Such technology might also have the ability to read human emotions through verbal and nonverbal communication, including changes in breathing, eye movement, blood pressure or voice.

What about the potential weaknesses of robots? Perhaps there will be none. While androids will learn how to express emotions such as sadness, joy, compassion and empathy when interacting with a target, they will not internalize them. As a result, they will not have any emotional vulnerabilities. They will be exclusively focused on executing the plan of their human taskmasters with extreme precision. As such, their human targets will continue to remain the weakest link in an organization's security.

Technology and the way social engineers use it will continue to evolve, while humans—along with their motivations, vulnerability and instinct to trust—will remain a constant. While organizations can't manage the myriad of AI-fueled schemes social engineers might use to manipulate a target in the future, they can do their best to make sure their security posture's weakest link remains its first line of defense.

From the Author

Thank you for reading *Confessions of a CIA Spy – The Art of Human Hacking*. If you enjoyed this book (or even if you didn't), please visit the site where you purchased it and write a brief review. Your feedback is important to me and will help other readers decide whether to read the book too.

If you'd like to learn more about human hacking, future book releases, speaking engagements and educational programs, please visit www.counterintelligence-institute.com.

Peter Warmka, 2021

Appendix A

Personal Assessment Questionnaire

The attached questionnaire should be used by a reader to assess their own security posture relevant to potential social engineering threats and ways to improve.

Protection of Personal Data – Part I

Please review all social media sites you use (LinkedIn, Facebook, Twitter, Instagram, YouTube, TikTok, etc.), as well as any other online resources (organizational websites, blogs, general Google search results) that may contain your personal information, whether indicated in your profile or revealed through photos and posts. Indicate below what information can be found online:

Date of Birth:
Birthday:
Place of Birth:
City where you currently live:
Actual address:
Posted email address:
Posted telephone number:
Your current location at this minute:
ID numbers from driver's license, passport or employee badge:
Academic degrees and where they were obtained:
Current academic studies:
Professional certifications:
Work history:
Current employer/position/responsibilities:
Any comments you made about your job:
Awards received:
Publications:
Charities you support:
Volunteer work:
Past travel:
Upcoming travel plans:
Favorite sports teams:
Favorite films/actors:
Favorite books:
Favorite food/beverage/restaurants:
Favorite stores:
Favorite music genre/artists/bands:
Hobbies:
Collections:
Favorite news outlets:
Other socioeconomic indicators, including:
    Club memberships:
    Attendance at high-profile events:
    Pictures displaying cars/boats/RVs/jewelry:
Children's private school:
Religion/religious events attended:
Political affiliation/political events attended/political views

expressed:

Sexual preferences:

Dating sites or apps used:

How are they linked to your name?

Any potentially compromising information?

Personal Relationships, including:

Significant other:

Children/names/ages:

Extended family members:

Identified circle of closest friends:

Identified professional contacts:

Mitigation: Realizing what information is now publicly exposed, think about how it could be used by a social engineer for gaining access to you, a family member, a colleague or your employer. Identify the most sensitive information and consider its removal or modification and maximize your privacy settings.

Protection of Personal Data – Part II

List the social media platforms you currently use or have used in the past and verify whether you have reviewed and updated their privacy settings. Consider having close family members also review their settings, as their accounts can be used to collect information on you.

Social Media SitePrivacy Setting Verified (Y/N)

_____

Protection of Personal Data – Part III

1. Identify all online accounts you use that require a username and password.
2. Identify how many of them are accessed using the same password.
3. How are you keeping track of them?
4. Are you keeping them written down?
5. Mitigation: Review various password managers and consider using one of them.

Vulnerability to Social Engineering Attempts

1. How confident are you that you could recognize someone's attempt to use elicitation techniques to gather sensitive information on you or your company?
2. If it were to occur, do you know what you would do?
3. Can you easily be targeted for an approach outside of

your office at establishments you routinely visit (cafes, restaurants, gyms, places of worship), at conferences, trade shows, social or professional association events?

4. Have you or anyone you know ever been contacted by a headhunter? If contacted in the future, what will you do to verify the legitimacy of the prospect?
5. What measures do you take to verify the legitimacy of an email requesting that you take an action such as clicking on a link or opening a document?
6. What measures do you take to verify the legitimacy of a text message received?
7. What measures do you take to verify the identity of a caller and the legitimacy of their request to obtain information or a request that you take a specific action?
8. What measures do you take to verify the legitimacy of someone who unexpectedly comes to your door offering a service or requesting donations?

Appendix B

Additional Resources

Provided in this appendix is a short list of available online resources recommended by the author for additional information on the topics discussed in this book.

Information is Beautiful – visualization of the world's biggest data breaches dating back to 2009

www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

Hackmageddon – detailed timeline of data breaches around the world

www.hackmageddon.com/category/security/cyber-attacks-timeline

Realtime Global Cyber Threats – presented by Kaspersky

www.cybermap.kaspersky.com

U.S. Department of Health and Human Services Breach Portal – impressive detail of all breaches of unsecured protected health information

www.ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Top 100+ Cyber Security Blogs & Infosec Resources – even more resources about the latest cybersecurity threats

www.ddosattackprotection.org/blog/cyber-security-blogs

Social Engineering – educational site specifically focused on social engineering

www.social-engineer.org

Glossary

Backstopping: Support obtained and used to add credence to a cover story or legend. It may be material such as business cards, websites or brick-and-mortar offices, or it can be a simple verification by someone answering a telephone number.

Business Email Compromise (BEC): This is an attack where the perpetrator gains access to the IT network of a target organization and electronically impersonates a senior official, providing fraudulent wire transfer instructions to an employee for execution.

Cover Story: Also referred to as a cover legend, it is a fictitious account of who the person claims to be and the purpose of their activity.

Dark Web: The portion of the internet within the deep web that is only accessible through special software, allowing users to remain anonymous. It is frequently used by the criminal world for the exchange of products, services and information.

Deep Web: The portion of the web that is not indexed and therefore not discoverable by means of standard search engines.

Elicitation: Methodology used by social engineers to extract sensitive information during a casual conversation with an unwitting target.

Human Hacking: Also referred to as social engineering, it is the art of manipulating people to undertake an activity that meets the objective of the hacker.

Insider: An employee or contractor who has unescorted access within an organization.

Malicious Insider: An employee or contractor who decides to cause financial or other harm to the organization.

Open-Source Intelligence (OSINT): Information that is publicly available.

Phishing: A common social engineering technique using an email to entice a recipient to click on a link or open an attachment, allowing for malware to be downloaded.

Pretext: Similar to a cover story, it is typically a false pretense used while engaging someone over the telephone.

Ransomware: Security breach attack by which the threat actor encrypts the target's data and holds it hostage until a ransom, usually in the form of bitcoin, is paid.

Smishing: Similar to phishing, it is a common social engineering technique using a SMS text message to entice a recipient to click on a link or open an attachment, allowing for malware to be downloaded.

Social Engineering: Also referred to as human hacking, it is the art of manipulating people to undertake an activity that meets the objective of the hacker.

Spear Phishing: An email that has been carefully crafted to target a specific individual.

State Actor: Someone conducting intelligence activities under the direction or interest of a nation state.

Surface Web: The portion of the internet that is indexed and accessible by standard search engines.

Vishing: The use of a telephone by a social engineer to gather information from a target or manipulate them to undertake a certain action.

About the Author

- Former Senior Intelligence Officer with the CIA with over 20 years of experience in breaching the security of organizations overseas
- Certified Protection Professional (CPP) and Certified Fraud Examiner (CFE)
- Founder of Orlando-based firm Counterintelligence Institute, LLC
- Adjunct Professor in Webster University's Master of Cyber Security Program
- Conference speaker, guest podcaster and author of numerous publications on social engineering and the manipulation of insiders
- Topics on which Peter can contribute his expertise: Identity Theft, Security Breaches, Social Engineering, Privacy versus Security, Social Media Profiling, Cyber Security, Espionage
- Passionate about using his expertise in helping city, state and federal government entities, nonprofits, academic institutes, private companies and individuals safeguard their sensitive proprietary and/or personal data

www.linkedin.com/in/peterwarmka/
www.counterintelligence-institute.com
www.facebook.com/counterintelligenceinstitute
www.twitter.com/the_cinstitute
www.youtube.com/channel/UC9xFgPIXmME8CIu5hzf3J-A

For additional information, please contact Peter directly:
pgwarmka@counterintelligence-institute.com